



Medical Care Services: Policies and Procedures

HIPAA Privacy Compliance Documentation

Publish Date: 7/22/05





Contents

Preface	xi
1 Introduction	1-1
Plan Management Branch (COHS, GMC, 2-Plan).....	1-1
<i>County Organized Health Systems</i>	1-1
<i>Geographic Managed Care</i>	1-2
<i>Two Plan Model</i>	1-2
Plan Monitoring/Member Rights Branch (Ombudsman)	1-3
Financial Unit.....	1-3
Medi-Cal Managed Care Contracted Health Plans.....	1-3
Medi-Cal Operations Division	1-4
Home and Community Based Services.....	1-4
Field Operations Support	1-6
Medi-Cal Policy Division	1-6
Medi-Cal Benefits Branch.....	1-6
Medi-Cal Eligibility Branch.....	1-6
Breast and Cervical Cancer Treatment Program	1-7
Rate Development Branch	1-7
Payment Systems Division	1-8
Headquarters Management Branch	1-9
Third Party Liability Branch	1-9
Office of Medi-Cal Dental Services Branch	1-9
Office of Medi-Cal Payment Systems.....	1-9
Management Information System – Decision Support System	1-10
Provider Enrollment Branch	1-10
Office of HIPAA Compliance	1-10
Fiscal Intermediary-IT Mgmt. Branch.....	1-10
Fiscal Intermediary-Operations Mgmt. Branch	1-11
Office of Medi-Cal Procurement	1-11
2 Individual Access	2-1
Overview	2-1

Policy	2-3
Information Accessible By the Individual or Personal Representative.....	2-3
Individuals Who May Access Medical Records	2-3
Conservators	2-4
Agents or Surrogates.....	2-4
Minors/Parent or Guardian.....	2-5
Deceased Individuals.....	2-6
Procedures	2-7
Requests for Access/Access Form	2-7
Verification of Individual Identity	2-7
Address Verification	2-8
Right to Inspect Records.....	2-8
Format of Information Provided.....	2-9
Time and Manner of Access to Records	2-9
Denial of Access to Records	2-10
No Right to Access/Not Subject to Review (45 C.F.R §164.524 (a) (2)).....	2-10
Denials of Access Subject To Review (45 C.F.R. §164.524 (a)(3))	2-10
Review of Denials by a Licensed Health Care Professional.....	2-11
Fees Charged for Access.....	2-12
Medi-Cal Records Available for Access	2-12
Telephone Request for Access	2-13
Individual Beneficiary	2-13
Legal Basis of Disclosures.....	2-13
Levels of Telephone Requests for Information	2-14
Level 1	2-14
Level 2.....	2-15
Level 3.....	2-15
Responding to Beneficiary Calls for Access to Records	2-15
Forms to be Sent.....	2-15
Third Party Liability Requests.....	2-16
Requests from Attorneys.....	2-16
Receipt of Request for Access	2-16
Fee-for-Service vs. Managed Care	2-17
Request for CDR Information Only.....	2-17
Request for CDR and TAR or Case Management Records	2-18
Request for TAR and/or Case Management With No CDR.....	2-18
Subpoena to the Medi-Cal Operations Division.....	2-18
Requests for CDR, TAR and/or Case Management Records	2-19

Definitions.....	2-19
Request for Access to PHI (DHS 6236).....	2-21
Request to Access PHI by Parent, Guardian or Personal Representative (DHS 6237).....	2-22
Authorization for Release of PHI (DHS 6247).....	2-23
3 Safeguards	3-1
Overview	3-1
Policy	3-2
Information Security Policy	3-3
Health Administrative Manual (HAM)	3-4
Access to Department Records – HAM Policy 11-3030.....	3-4
Security of Confidential Information – HAM Policy 11-3060.....	3-4
Procedures	3-5
Administrative Safeguards	3-5
Technical Safeguards	3-5
Computer Passwords.....	3-6
Computer Monitors	3-6
Computers Peripherals	3-6
Laptop Computers	3-7
Physical Safeguards	3-8
Paper Files.....	3-8
Removing Records from a DHS Facility.....	3-9
Faxes.....	3-9
Mail	3-10
Oral Communications	3-11
4 Uses and Disclosures.....	4-1
Overview	4-1
Policy	4-2
Uses and Disclosures for the Medi-Cal Program	4-3
Definition of Use and Disclosure	4-3
Disclosures for Limited Purposes.....	4-4
Authorizations for Use and Disclosure	4-4
Use and Disclosure for Treatment, Payment, and Operations (TPO)	4-5
Uses and Disclosures to Business Associates.....	4-6
The Minimum Necessary PHI to Be Used or Disclosed	4-6

Uses and Disclosures to Health Oversight Agencies	4-6
Uses and Disclosures in Judicial Proceedings	4-7
Procedures	4-7
Definitions.....	4-8
5 Minimum Necessary	5-1
Overview	5-1
Policy.....	5-2
Procedures	5-3
Use of PHI within Department of Health Services	5-3
Disclosures of PHI.....	5-4
Public Officials	5-4
Disclosures to Other Covered Entities	5-4
Business Associates	5-5
Research	5-5
Required by Law	5-5
Public Health or Health Oversight/As Required By Law	5-5
Documentation	5-6
Program Management Responsibilities.....	5-6
Definitions.....	5-7
6 Request Restriction of Uses or Disclosures of Protected Health Information.....	6-1
Overview	6-1
Policy.....	6-2
Procedures	6-2
Process to Request Restriction of Uses and Disclosures of PHI.....	6-2
Agreeing to Restriction of Use and Disclosures of PHI	6-3
DHS is Not Required to Agree With the Restriction Requested By an Individual.....	6-4
Termination of Restriction of Use and Disclosure of PHI	6-4
Definitions.....	6-5
Request to Restrict Use and Disclosure of PHI (DHS 6240)	6-7
Request to Restrict Use and Disclosure of PHI by Parent, Guardian or Personal Representative (DHS 6241)	6-8

7 Business Associate Relationships.....	7-1
Overview	7-1
Policy	7-3
Procedures	7-3
Identifying and Tracking DHS Business Associates	7-3
Compliance Dates	7-3
Required Terms and Conditions.....	7-4
Business Associate is Another Government Entity	7-5
Business Associate Non-Compliance	7-6
Response to Business Associate Inappropriate Uses or Disclosures	7-6
Definitions.....	7-7
8 Accounting of Disclosures.....	8-1
Overview	8-1
Policy	8-2
Accountable Disclosures	8-3
Allowable Disclosures	8-3
Time Period for the Accounting of Disclosures.....	8-3
Content of the Accounting of Disclosures	8-4
Procedures	8-4
Requesting an Accounting of Disclosures	8-4
Verification of Individual Identity	8-5
Address Verification	8-5
Provision of the Accounting.....	8-6
Fees for the Accounting of Disclosures	8-6
Documentation	8-6
Suspension of the Right to Receive an Accounting of Disclosures	8-7
Format for Maintaining an Accounting of Disclosures	8-7
Alternative Systems for Tracking Data	8-7
Staff Assigned to Oversee Accounting of Disclosures	8-8
Multiple Disclosures	8-8
Disclosures for Research	8-8
Definitions.....	8-9
Accounting of Disclosures Log	8-10
Request for an Accounting of Disclosures of PHI (DHS 6244)	8-11

Request for an Accounting of Disclosures of PHI by Parent, Guardian or Personal Representative (DHS 6245)	8-12
---	------

9 Amending Protected Health Information9-1

Overview	9-1
Policy	9-2
Procedures	9-2
Timely Action.....	9-2
Verification of Individual Identity of Requester	9-2
Personal Representative Request.....	9-3
Address Verification	9-3
Denying the Amendment.....	9-4
Review of Refusal to Amend Record	9-5
Statement of Disagreement of Requester	9-5
Rebuttal Statement	9-5
Amendments Forwarded by Prior Covered Entities	9-5
Definitions.....	9-5
Request to Amend PHI (DHS 6238)	9-7
Request to Amend PHI by Parent, Guardian or Personal Representative (DHS 6239).....	9-8

10 Confidential Communications 10-1

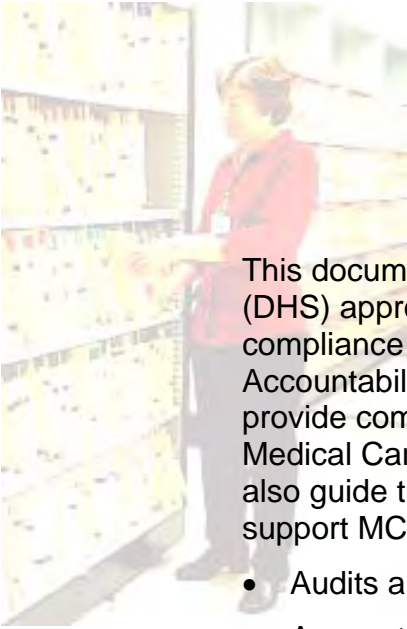
Overview	10-1
Policy	10-2
Procedures	10-2
Requesting Confidential Communications	10-2
Alternative Address and/or Alternative Telephone Number Request	10-3
Alternative Means of Contact	10-3
Approving or Denying the Request	10-3
Definitions.....	10-4
Confidential Communication Request (DHS 6235).....	10-5

11 Complaints 11-1

Overview	11-1
Policy	11-2

Procedures	11-2
Who May File a Complaint	11-2
Time Limits for Filing Complaints	11-3
Complaint Forms	11-3
Submitting the Complaint	11-4
Initial Analysis and Routing of the Complaint	11-4
Investigating and Resolving Complaints	11-5
Status Log	11-6
Retaliation	11-6
Documentation	11-7
Definitions	11-7
Privacy Complaint Form (DHS 6242)	11-8
Whistleblower Complaint Form (DHS 6243)	11-9
12 Privacy Breach	12-1
Overview	12-1
Policy	12-2
Procedures	12-2
Who May Notify of a Breach	12-2
Breach Notification Process	12-2
Initial Analysis of the Breach	12-3
Investigating and Resolving Breaches	12-4
Retaliation	12-5
Documentation	12-5
Definitions	12-6
13 Training	13-1
Overview	13-1
Policy	13-1
Mandatory Training Information	13-2
Changes to Privacy Policies and Procedures	13-2
Procedures	13-3
Method of Training	13-3
Content of Training	13-3
Documentation to be Maintained	13-4
Definitions	13-5

14 Employee Sanctions	14-1
Overview	14-1
Policy	14-1
Procedures	14-2
Violations.....	14-2
Tracking Privacy Violations and Applied Sanctions.....	14-2
Responsibilities of Managers and Supervisors.....	14-2
Training and Certification	14-3
Criminal and Civil Penalties.....	14-3
 Appendix	 A-1



Preface

This document presents the Department of Health Services (DHS) approved Privacy Policies and Procedures for compliance with the Health Insurance Portability and Accountability Act (HIPAA). These policies and procedures provide compliance guidance to all units and programs within Medical Care Services (MCS). These policies and procedures also guide the privacy functions of the DHS programs that support MCS including:

- Audits and Investigations;
- Accounting;
- Office of Legal Services;
- ITSD;
- Medi-Cal Fraud Prevention; and
- Fiscal Forecasting and Data Management Branch.

The following Privacy Policies and Procedures apply to **all** DHS staff members who work in MCS **and** in units and programs that support MCS:

- Accounting of Disclosures;
- Business Associates;
- Complaints;
- Employee Sanctions;
- Minimum Necessary;
- Privacy Breach;
- Safeguards;
- Training;
- Uses and Disclosures.



1 Introduction

Medical Care Services (MCS) directly operates California's Medicaid program (Medi-Cal) and the program's eligibility, scope of benefits, reimbursement, and other related components. MCS is responsible for the Department of Health Services (DHS) fiscal intermediary contract that pays claims for Medi-Cal.

Medi-Cal Managed Care Division (MMCD)

MMCD is responsible for establishing networks of organized managed care systems which emphasize primary and preventive care in order to improve beneficiary access and quality of care, and to ensure cost-effective use of health care resources. Under managed care, health care providers receive a fixed rate capitation for providing a beneficiary's comprehensive care. In contrast, under the fee-for-service (FFS) system the provider bills for each specific service provided. Beneficiaries enrolled in a managed care plan select a primary care physician who provides their health care services on a regular basis and refers them to specialists when medically necessary.

Plan Management Branch (COHS, GMC, 2-Plan)

The Plan Management Branch (PMB) has three main contract categories: County Organized Health Systems (COHS), Geographic Managed Care, and Two-Plan.

County Organized Health Systems

Under a COHS, a County Board of Supervisors creates a local agency, with representation from providers, beneficiaries, local government, and other interested parties, to contract with the Medi-Cal program.

Operating under federal Medicaid freedom of choice and other waivers, the COHS administer a capitated, comprehensive, case-managed health care delivery system. This system has responsibilities for utilization control and claims administration and Medi-Cal covered health care services to all Medi-Cal

beneficiaries who are legal residents of the county. Beneficiaries are given a wide choice of managed care providers but do not have the option of obtaining Medi-Cal services under the traditional FFS system.

Geographic Managed Care

Under Geographic Managed Care (GMC), covered beneficiaries are informed at the county welfare department about the available managed care health plans and indicate their choice about receiving Medi-Cal services. Aged, blind and disabled beneficiaries eligible for Medi-Cal under the Supplemental Security Income program may voluntarily enroll in one of the managed care health plans or choose to retain their health care benefits through the FFS system.

Sacramento County was selected for the development of a GMC project in early 1992, with the project starting on April 1, 1994.

Under GMC, the DHS entered into contracts with seven managed care health plans and found dental plans to cover the entire (formerly known as) Aid for Families with Dependent Children-linked population in Sacramento County on a mandatory enrollment basis. DHS received federal waivers that permitted provision of Medi-Cal benefits to this population exclusively through managed care health plans. In 1994, San Diego County requested and started the state's second GMC project.

Two Plan Model

Under the DHS plan for expansion of managed care in each of the 12 regions designated for expansion, DHS is contracting with one locally developed comprehensive managed care system (referred to as the Local Initiative) and one non-governmental-operated Health Maintenance Organization (HMO) (referred to as the Commercial Plan). Beneficiaries in the 12 regions are given a choice between these two health care plans. Both plans are responsible for providing or arranging for all covered health care services for the majority of Medi-Cal beneficiaries in the region on a capitated, full-risk basis. The 12 counties targeted for expansion are: Alameda, Contra Costa, Fresno, Kern, Los Angeles, Riverside, San Bernardino, San Francisco, San Joaquin, Santa Clara, Stanislaus, and Tulare.

Plan Monitoring/Member Rights Branch (Ombudsman)

This unit documents and monitors suspected fraud cases resulting in possible Medi-Cal provider suspension and/or recoupment of monies paid. Cases are opened based on beneficiary calls to Denti-Cal, Medi-Cal hotline, Department of Justice (DOJ) toll free line, local district attorneys, other providers, and concerned citizens. Reports are also run, data-mined, to look for statistical outliers.

Financial Unit

The Financial Unit is responsible for processing the capitation payments, risk payments and/or financial payments for all health plans under Managed Care. This process is done at the beginning of the month for capitation payments. The Financial Unit is responsible for ensuring the payments are in compliance with the contract and time frames. They also work closely with the Accounting Unit.

Medi-Cal Managed Care Contracted Health Plans

The contracted health plans have certain responsibilities to Medi-Cal Managed Care regarding HIPAA Compliance, which are enumerated in a HIPAA addendum to their contracts.

- **Prohibition of External Disclosure of Lists of Beneficiaries.**
A health plan must give its assigned DHS contract manager a list of external entities, including persons, organizations, and agencies, other than DHS, which are not part of its treatment network, to which it discloses lists of Medi-Cal beneficiary names and addresses. This must occur within 30 days of the execution of the contract between the health plan and DHS and annually thereafter.
- **Reporting of Improper Disclosures**
Improper disclosures must be reported to the contract manager within twenty-four (24) hours during a work week, of discovery by contractor that protected health information (PHI) has been used or disclosed other than as provided for by the contract or otherwise in violation of HIPAA regulations, or other statutes and regulations pertaining to privacy and security of PHI.

- **Notification of Breach**

Notice must be given to the contract manager, the DHS Privacy Officer and the DHS Information Security Officer within one hour (1) hour of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable Federal and State laws or regulations.

A health plan should investigate such breach, or unauthorized use or disclosure of PHI, and provide a written report of the investigation to the DHS Privacy Officer within ten (10) working days of the discovery of the breach or unauthorized use.

Medi-Cal Operations Division

Medi-Cal Operations Division (MCOD) provides timely adjudication of Treatment Authorization Requests (TAR), oversees several medically related programs, and case manages California's most medically fragile population.

In California, certain high cost medical procedures/services and drugs require the review and approval of State employed physicians, nurses, pharmacists, or trained technicians prior to payment for services rendered to Medicaid (known as Medi-Cal in California) and County Medical Services Program (CMSP) patients to ensure the patient receives the medically appropriate services. In addition, MCO is charged with the oversight and monitoring of a number of related Medi-Cal programs.

MCOD has over 580 State employees working in the field offices and two pharmacy sections throughout the State and in the Headquarters Office in Sacramento. MCO Headquarters staff handles the administrative and related functions for the MCO.

MCOD is divided into two primary sections, Home and Community Based Services and Field Operations Support.

Home and Community Based Services

The Home and Community-Based Services (HCBS) Branch has the responsibility for the management of select home and community-based services under the Medi-Cal program. These

services include federally funded waivers and select services under the Medi-Cal program. All programs under the HCBS Branch have been coordinated with other initiatives under the California Health and Human Services Agency's Long Term Care Council and are included as components of the California Olmstead Plan that was submitted to the Legislature in May 2003. The HCBS Branch is comprised of two sections, the In Home Operations Section and the Monitoring and Oversight Section.

The In Home Operations Section is responsible for the administration and authorization of services listed under the In Home Medical Care (IHMC) and Nursing Facility (NF) Waivers as well as the authorization of select Early Periodic Screening, Diagnosis and Treatment (EPSDT) services.

The Monitoring and Oversight Section is responsible for the monitoring and oversight of the Developmentally Disabled (DD) and Multipurpose Senior Services Program (MSSP) Waiver; management of a 1915(b) freedom of choice Waiver; and the implementation of the Assisted Living Waiver Pilot Project. The Monitoring and Oversight Section (MOS) of the HCBS Branch is responsible for the indirect management of two pilot projects and two waivers:

- Intermediate Care Facility for the Developmentally Disabled-Continuous Nursing (ICF/DD-CN) Pilot Project
- Assisted Living Waiver Pilot Project (ALWPP)
- Developmentally Disabled (DD) Waiver
- Multipurpose Senior Services Program (MSSP) waiver

Field Operations Support

The Field Offices process the TARs submitted by Medi-Cal providers for Core Services and Regionalized Services throughout the State.

The Southern Field Operations Branch consists of three field offices located in Los Angeles, San Bernardino, San Diego, and one Pharmacy Section (located in Los Angeles). The Northern Field Operations Branch also consists of three field offices located in Fresno, Sacramento, San Francisco, and one Pharmacy Section (located in Stockton) and Medical Case Management.

Field Operations also includes Appeals & Litigation, Administrative Unit, Hospital Contracts and Sub-acute.

Medi-Cal Policy Division

The Medi-Cal Policy Division (MCPD) is responsible for administering the policy development, interpretation, and implementation of the State's Medi-Cal program in the determination of program eligibility, program benefits, and program rate provisions.

The MCPD consists of the following branches and sections.

Medi-Cal Benefits Branch

The Medi-Cal Benefits Branch provides policy development and recommendations regarding the scope, quality and methods of providing Medi-Cal benefits. The Benefits Branch develops and implements regulations and procedures related to the scope and duration of benefits and the circumstances under which medical benefits will be covered. Medi-Cal covers a wide range of services.

Medi-Cal Eligibility Branch

The Medi-Cal Eligibility Branch is responsible for the coordination, clarification, and implementation of Medi-Cal regulations, policy, and procedures to assure that Medi-Cal eligibility is determined accurately and on a timely basis by the 58 county public social services agencies.

Breast and Cervical Cancer Treatment Program

On August 10, 2001, Assembly Bill 430 was chaptered into law, authorizing the State to implement the new Breast and Cervical Cancer Treatment Program (BCCTP). The DHS implemented the BCCTP on January 1, 2002. Under this new program, low-income California residents who have breast and/or cervical cancer can enroll at a doctor's office to receive no-cost cancer treatment coverage.

The BCCTP is the first program in the nation to grant same-day, full-scope Medicaid (Medi-Cal in California) from the doctor's office through an Internet-based application and eligibility determination process.

The doctors participating in this program can screen, diagnose or confirm a diagnosis of breast and/or cervical cancer and enroll individuals in BCCTP.

Enrolling doctors submit an Internet-based application to the State to enroll eligible individuals who are diagnosed with, and are in need of treatment for, breast and/or cervical cancer.

The BCCTP also includes a State-only program that provides cancer treatment and cancer-related services only to persons who are screened and are found to be in need of treatment for breast and/or cervical cancer. The State-only program provides 18 months of coverage for breast cancer treatment and 24 months of coverage for cervical cancer treatment.

Rate Development Branch

The Rate Development Branch establishes the provider payment schedule for covered services, conducts rate studies, develops and implements systems to constrain the rate of increase of Medi-Cal hospital inpatient costs and reimbursements, and develops capitation rates for prepaid health plans and organized health systems. The Rate Development Branch also provides administrative oversight for six home and community-based services waivers, two demonstration project waivers, and three freedom of choice waivers. The Rate Development Branch consists of three sections:

- Hospital Finance and Capitation Section - The Hospital Finance & Capitation Section (HFCS) oversees all functions of the Disproportionate Share Hospital (DSH) (Senate Bill

855) program, the Hospital Recoupment (HRU) program, and the Capitation Rates (CRU) program.

- **Provider Rate Section** - The Provider Rate Section (PRS) is responsible for complex and sensitive rate-setting studies that involve statistical analyses, grouping methodologies, and reimbursement modeling. The purpose of these studies is to establish an evidentiary basis for setting maximum reimbursement rates for services provided to individuals eligible under Medi-Cal, California Children Services, and other state programs.
- **Waiver Analysis Section** - The Waiver Analysis Section (WAS) provides administrative oversight for 11 Medicaid waivers with regard to policy development, implementation, interpretation, and compliance. WAS is the primary liaison with the Centers for Medicare and Medicaid Services (CMS) for the 11 assigned waivers and provides policy consultation and technical assistance to the programs that operate the waivers.

Payment Systems Division

Payment Systems Division's (PSD) mission is the overall administration, oversight and monitoring of the Medi-Cal fiscal intermediary (FI) contracts, which maintain Medicaid Management Information Systems (MMIS) for both the medical and dental programs. PSD also ensures that Medi-Cal is the payer of last resort. In addition, PSD ensures effective administration, oversight and monitoring of the Medi-Cal managed care enrollment broker contract.

The main function of PSD are:

- Manages the FI's MMIS claims processing operations and reports.
- Oversees the development and implementation of system changes and modifications.
- Develops policies and procedures governing claims adjudication.
- Negotiates changes to the FI contracts.
- Enrolls providers.
- Adjudicates provider appeals.

- Develops policies and procedures for the Denti-Cal program.
- Monitors the dental managed care program.
- Identifies and utilizes third party payers in lieu of expending State funds for Medi-Cal services.
- Administers and oversees the managed care beneficiary enrollment broker activities. (Health Care Options)

The PSD includes the following areas.

Headquarters Management Branch

Headquarters Management Branch's (HMB) mission is to provide customer service to all providers who serve Medi-Cal beneficiaries to assure that their claims are paid accurately and timely by responding to their questions and concerns.

Third Party Liability Branch

The Third Party Liability Branch (TPL) is charged with the responsibility of ensuring that the Medi-Cal program complies with state and federal laws and regulations relating to the legal liability of third parties for health care services to beneficiaries, and of taking all reasonable measures to ensure that the Medi-Cal program is the payer of last resort.

Office of Medi-Cal Dental Services Branch

The Medi-Cal Dental Program oversees dental programs administered through the FFS fiscal intermediary and/or through dental managed care contracts.

Office of Medi-Cal Payment Systems

The Office of Medi-Cal Payment Systems (OMPS) enables the MCS program to improve the health of Californians by providing and supporting secure and effective Information Technology (IT) solutions and empowering MCS staff to make optimum use of IT tools and resources in meeting their individual mission objectives.

Management Information System – Decision Support System

The Management Information System - Decision Support System project is to establish a comprehensive information system to support the day-to-day program and contract management needs of Medi-Cal.

Provider Enrollment Branch

The Provider Enrollment Branch (PEB) is responsible for the enrollment and re-enrollment of FFS health care service providers into the Medi-Cal program.

Office of HIPAA Compliance

HIPAA is designed to streamline health care delivery by employing standardized, electronic transmission of administrative and financial transactions, along with protection of confidential health information.

Fiscal Intermediary-IT Mgmt. Branch

The Fiscal Intermediary-IT Mgmt. Branch (FI-ITMB) mission is to improve the health of all Californians by analyzing, planning, and developing timely and cost effective changes to the CA-MMIS operations, providing data processing support to the Department in Medi-Cal fraud detection and cost containment activities. The FI-ITMB also answers inquiries concerning claims payment policies and procedures from providers, provider associations, the Legislature, other state and federal agencies, and the general public.

The main functions of the FI-ITMB are:

- Manage portions of the FI contract and perform contract compliance oversight.
- Oversee the FI operations in relation to claims processed by the California Medicaid Management Information System (CA-MMIS).
- Direct the FI on claims processing payment policies and procedures. Design, develop, and implement enhancements and other modifications to CA-MMIS as a result of policy changes, legislation, lawsuits, or administrative efficiencies.

Perform monitoring and maintenance activities on CA-MMIS to validate the integrity and accuracy of the system.

Fiscal Intermediary-Operations Mgmt. Branch

The Fiscal Intermediary Operations Management Branch (FI-OMB) mission is to protect and improve the health of all Californians by ensuring the provision of complete, accurate and timely service to customers of the CA-MMIS claims processing system, and to interpret and implement medical policies into the CA-MMIS while ensuring the integrity of the claims processing system. Additionally, FI-OMB works to reduce fraudulent provider billings and implements cost savings processes that reduce fee-for-service Medi-Cal program expenditures and ensure accountability to control agencies for CA-MMIS operations.

The main functions of FI-OMB are:

- Oversee provider claims assistance activities including both the quality and timeliness of information given regarding Medi-Cal billing and claims processing.
- Direct the FI contractor on CA-MMIS customer relations including provider education and outreach, Internet information services, and publications.
- Ensure that medical policies are translated accurately and implemented in a timely manner into the CA-MMIS claims processing system.
- Direct the FI contractor in the performance of anti-fraud actions, activities and measurements.

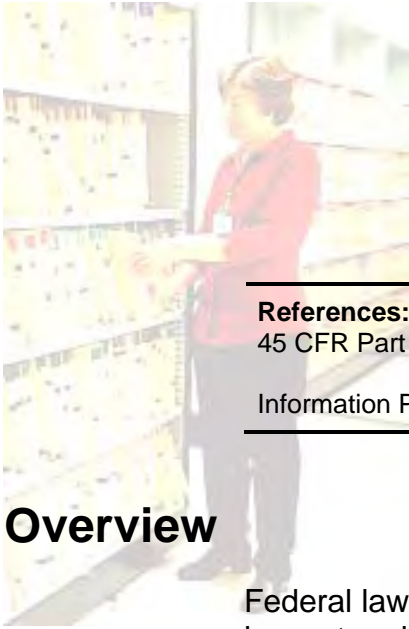
Office of Medi-Cal Procurement

The Office of Medi-Cal Procurement (OMCP) was established to serve as an internal consulting and advisory group within the DHS to perform major procurements conducted by the Medi-Cal program. The goal of the OMCP is to ensure that Medi-Cal contracting and procurement procedures are of the highest integrity, and that the competitive bidding processes are employed to the maximum extent required by law.

- Oversee and facilitate cost containment projects that result in program cost reductions by reducing payments to

providers with inappropriate billing practices or by implementing improvements to claims processing operations.

Provide support for control agency reviews and audits of the CA-MMIS contract and claims processing activities.



2 Individual Access

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part §164.524

Information Practices Act (IPA) Ca. Civil Code §§1798.32-1798.34

Overview

Federal law requires that individuals have a right of access to inspect and obtain a copy of their protected health information (PHI) in a designated record set (DRS), for as long as the health information is maintained by the Medi-Cal program or its business associates. There are limited exceptions to an individual's right to access PHI.

The IPA also gives individuals the right to access their health records in the possession of state agencies. (Ca. Civil Code §§1798.32-1798.34)

Requests for access to Medi-Cal beneficiary records come into Department of Health Services (DHS) through:

- Medi-Cal Operations Division (MCOD) and Electronic Data Services (EDS);
- Privacy Office phone tree;
- Privacy Officer correspondences;
- Subpoena requests to MCOs;
- Estate recovery, personal injury, or workers' compensation requests to Third Party Liability (TPL).

Documents requested may include:

- Claim Detail Reports (CDRs);
- Treatment Authorization Requests (TARs);
- Case Management Records;
- Managed Care Records;
- Enrollment;
- Disenrollment;

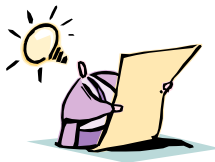
- Capitation Payments; and
- Complaint Investigations.

This section explains the process to allow individuals to access their PHI. The Individual Access Section includes information pertaining to:

- Information Accessible by Individual or Personal Representative;
- Individuals Who May Access Medical Records;
- Minor Consent;
- Request for Access/Access Forms (DHS 6236 and 6237);
- Verification of Individual Identity;
- Address Verification;
- Right to Inspect Records;
- Format of Information Provided;
- Time and Manner of Access to Records;
- Denial of Access to Record;
- Review of Denials by Licensed Health Care Professional;
- Fees Charged for Access;
- Medi-Cal Records Available for Access;
- Medi-Cal Request for Access Procedures;
 - Telephone Requests for Access
 - Responding to Beneficiary Calls for Access to Records
 - Forms to be Sent
 - TPL Requests
 - Requests from Attorneys
 - Receipt of Request for Access
 - Fee-for-Service vs. Managed Care
 - Requests for CDR Information Only
 - Requests for CDR and TAR or Case Management Records
 - Requests for TAR and/or Case Management With No CDR
 - Subpoena to the MCO

- Requests for CDR, TAR and/or Case Management Records
- Definitions;
- Request for Access to Protected Health Information (DHS 6236);
- Request to Access Protected Health Information by Parent, Guardian or Personal Representative (DHS 6237); and
- Authorization for Release of Protected Health Information (DHS 6247).

Policy



The policy of the Medi-Cal program is to provide individuals their right to access, to inspect and to obtain a copy of their PHI under the law.

Information Accessible By the Individual or Personal Representative

Generally, individuals have the right to access any health information used, in whole or in part, to make decisions about them.

Access is limited to the information contained in the DRS. The DRS is the group of records maintained by or for a health plan or provider that includes medical and billing records. Specifically, the DRS includes information regarding enrollment, payment, claims adjudication, and case or medical management records systems of Medi-Cal. Medi-Cal must identify and document the information contained in its DRS. Examples of information excluded from the DRS may be peer review documents, audits by oversight agencies, records compiled in reasonable anticipation of, or use in a criminal, civil or administrative action or proceeding.

Individuals Who May Access Medical Records

Under federal law, individuals, personal representatives of individuals, including the parents of minors, and minors themselves may have the right to access PHI.

Under the IPA an individual may designate another person of the individual's own choosing to inspect and obtain a copy of health records. (Ca. Civil Code §1798.34)

1. Individual is defined as the person who is the subject of the PHI.
2. Personal Representative - If under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, Medi-Cal must treat such a person as a personal representative with respect to the individual's PHI. Such personal representatives will be treated like the individual with regard to access to the relevant information.

The following categories of persons may have authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care.

Conservators

A person who is adjudicated to lack the capacity to make health care decisions may have a conservator appointed by court order. You should look at the certified letters of conservatorship to find out whether an individual has been determined to lack the capacity to make health care decisions and whether the conservator has authority to make medical decisions for the conservatee. (See Probate Code §§1880-1898 and 2353-2357)

Agents or Surrogates

An adult having capacity may execute a power of attorney for health care. The power of attorney for health care may authorize another person, called an agent, to make health care decisions on behalf of the individual if the individual becomes incapable of making his or her own decision or if the individual wants someone else to make those decisions. An adult may also designate another adult as a surrogate to make health care decisions for him or her by personally informing the supervising health care provider. This oral designation only is effective during the course of treatment or illness or during the stay in the health care institution. A person then authorized to make health care decisions for an individual has the same rights as the patient to request, receive, examine, copy, and consent to the disclosure of medical or any other health care information. (See the Health Care Decisions Law, Probate Code §§4600-4805.)

Please note that Medi-Cal may elect not to treat a person as a personal representative for purposes of access to an individual's records if Medi-Cal has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by the personal representative; treating such person as the personal representative could endanger the individual; or it is not in the best interest of the individual to treat the person as the individual's personal representative.

Minors/Parent or Guardian

A person under the age of 18 is generally unable to consent to medical treatment. If under applicable law a parent, guardian, or other person acting in place of the parent has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, Medi-Cal must treat such person as the personal representative of the child. However, minors have the right to access information about health care services to which they may consent under the law ("minor consent services"). A parent, guardian, or other person acting in place of the parent may agree to confidentiality between a covered health care provider and the minor with respect to a health care service. In this case, the minor has the right to access his or her own records.

Please note that state laws, including case law, should be examined by Medi-Cal with regard to the disclosure of information about an unemancipated minor to the minor, and/or to a parent, guardian, or other person acting in place of the parents.

If a parent, guardian, or other person acting in place of the parent requests access to the minor's PHI for minor consent services, the following rules apply. The parent, guardian or other person acting in place of the parent may not obtain access to the records unless:

- The minor requests that the parent, guardian, or other person acting in place of the parent have access; or
- State law permits or requires such access; or
- State law is silent on granting access and a licensed health care professional determines that the parent, guardian, or other person acting in place of the parent, who requests access to the minor's PHI, should have access to the records.

The following State laws pertain to minor consent services:

Children age 15 or older may consent for medical care when they are living separate from their parents and managing their own financial affairs. A physician or dentist may advise the minor's parent or guardian of the treatment if the whereabouts of the parent or guardian are known. (Family Code §6922)

A minor 12 years of age or older, who seeks or receives mental health treatment or counseling on an outpatient basis, or from a residential shelter can consent and have access to his or her PHI. A residential shelter must make efforts to notify the parent or guardian of the services. The involvement of the parent or guardian in the mental health treatment of the minor is up to the judgment of the professional treating the minor. (Family Code §6924)

A minor seeking pregnancy care or prevention of pregnancy can consent to his or her health care and have access to these records. Sterilization and abortion require the consent of the parent or guardian, except that a minor may petition the juvenile court for an abortion. (Family Code §6925)

A minor who alleges to have been sexually assaulted or raped may consent to and access his or her own health care information with regard to such care. A provider should try to contact the parent or guardian in a sexual assault case, unless the parent or guardian is the suspected perpetrator. (Family Code §§6927 and 6928)

A minor 12 years of age or older, who seeks care for drug or alcohol related problems may consent and access his or her own health information with regard to such care. (Family Code §6929)

Deceased Individuals

The PHI of a deceased individual is subject to the federal HIPAA privacy provisions for as long as Medi-Cal maintains the PHI. Executors, administrators or other persons having the authority to act on behalf of deceased individuals or their estate based on applicable laws must be treated as personal representatives. Access to PHI by these representatives is limited to information necessary to the function of the personal representative.

Procedures



The following procedures govern individual access to Medi-Cal records.

Requests for Access/Access Form

All requests for access to individual health information must be made **in writing** using the Medi-Cal Request for Access Forms, DHS 6236 (for the individual) and 6237 (for the personal representative). Each DHS health plan should document the process for providing access to its health plan beneficiaries, which should include the titles of persons or offices responsible for receiving and processing requests for access by individuals.

Many of the DHS health plan beneficiaries and provider patients will be directed by their Notices of Privacy Practices to contact the Privacy Office at (916) 445-4646 for information regarding their privacy rights, including access to their health information. For Medi-Cal, the phone line goes to EDS, where the EDS telephone staff field requests for access.

Verification of Individual Identity

In order to ensure that Medi-Cal is protecting individual health information, individuals requesting to inspect and copy records must verify their identities. Individuals will be requested to include their beneficiary ID number, date of birth, and date of death, in probate cases. **A request for access must also be accompanied by a photocopy of the California driver's license, an identification card issued by the Department of Motor Vehicles, or any other document that appears to be valid and establishes identity.** It is up to the individual program person designated to process access requests to verify the identity of individuals requesting access to their own records. Documents containing signatures are preferable, since the signature on the request form may be checked against the identification card. The following additional documents may be considered:

- Copy of the Individual's Birth Certificate;
- Beneficiary Identification Card;

- Managed Care Card; or
- State or Federal Employee ID Card/Check Cashing ID Card.

A notarized signature may be provided in lieu of a copy of one of the listed identifiers.

When a personal representative requests access to records of an individual, his or her legal authority to make medical decisions must be verified as well as his or her identity, using the above process. Verification of legal authority to make health care decisions would include documentation establishing conservatorship, legal guardianship, or power of attorney for health care decision-making. For a natural parent of a minor child, a birth certificate should suffice. If the parents are divorced proof of custody must be provided. A copy of the death certificate should be required for access to the records of decedents, as well as proof of executorships of the will/ administration of the estate. If there is no will and/or no probate, proof that the requestor is next of kin of the decedent may suffice.

Address Verification

Individuals requesting to be sent copies of records by mail must also verify their address. Requestors must include proof of their address such as a recent electricity, gas or phone bill, driver's license, rent receipt, or other documentation showing the requestor's name and address.

Right to Inspect Records

In addition to the right to request a copy of their health record, individuals may choose to inspect their records without cost. Under the IPA, inspection of records must be provided at a location near the residence of the individual or by mail, whenever reasonable.

Individuals may designate a person of their choosing to inspect the records. This should apply to in-person inspections. Records should generally be mailed to the address of the requesting individual, for security reasons. However, records may be mailed to attorneys for Medi-Cal beneficiaries, on request.

As most Medi-Cal programs are headquartered in Sacramento, a convenient location for inspection of records will not be

available for most requestors. Whenever a location near the residence of the individual is unavailable, Medi-Cal will copy and mail the information requested. Programs may choose to bill for postage.

Format of Information Provided

Medi-Cal must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format. If not available or readily producible in the requested format, Medi-Cal must provide a readable hard copy form or other form or format as agreed to by Medi-Cal and the individual.

Medi-Cal may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to such a summary or explanation; and the individual agrees in advance to the fees imposed, if any, by Medi-Cal for such summary or explanation.

Medi-Cal must, in disclosing information, delete confidential information relating to another individual, which may be contained in the record.

Time and Manner of Access to Records

Medi-Cal must provide the access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request.

Medi-Cal must act on a request for information that is readily accessible within 30 days after receipt of the request from the individual or his or her representative. If the request is granted, in whole or in part, Medi-Cal must inform the individual of acceptance and provide the access requested. If the request is denied, in whole or part, Medi-Cal must provide the individual with a written denial according to the criteria for denial of access. If the request is for PHI that is not maintained or readily accessible on-site, Medi-Cal must inform the individual of acceptance of the request, but has 60 days from the receipt of the request to act on it.

When the individual has inspected the records, copies of all or part of the record inspected should be provided within 15 days of the inspection, when requested. (Civil Code §§1798.34 (b))

Denial of Access to Records

Medi-Cal can deny access in the following categories: (A) No right to Access/Not Subject to Review and (B) Denial of Access/Subject to Review by a Health Care Professional.

No Right to Access/Not Subject to Review (45 C.F.R §164.524 (a) (2))

An individual does not have the right to access:

- Psychotherapy notes;
- PHI compiled in anticipation of, or for use in, civil criminal, or administrative actions or proceedings;
- PHI maintained by Medi-Cal that is subject to or exempt from certain provisions of the Clinical Laboratory Improvements Amendments (CLIA) of 1988;
- PHI requested by an inmate, maintained by a correctional institution, or by a provider on behalf of the correctional institution, if obtaining the information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate; or
- PHI obtained from someone else, other than a health care provider, under a promise of confidentiality, but only if access would be reasonably likely to reveal the source of the information.

Denials of Access Subject To Review (45 C.F.R. §164.524 (a)(3))

- Medi-Cal may deny access when a licensed health care professional determines, in the exercise of professional judgment, that the access is reasonably likely to endanger the life or physical safety of the individual or another person;
- The PHI makes reference to another person, and a licensed health care professional, in his or her professional judgment,

determines that access is reasonably likely to cause substantial harm to such person; and

- The request for access is made by the individual's personal representative, and a licensed health care professional, in his or her professional judgment, determines that access by such personal representative is reasonably likely to cause substantial harm to the individual or another person.

When Medi-Cal denies access, in whole or in part, it must:

- Give the individual access to any other PHI requested, after excluding the PHI which Medi-Cal has a ground to deny;
- Give the individual a timely written denial;
- The denial must be in plain language and contain the basis for denial, a statement as to whether the denial is subject to further review including how this right may be exercised;
- A description of how the individual may submit a complaint to Medi-Cal or the Secretary of Health and Human Services—including the name, title, and telephone number of the contact person or office; and
- If Medi-Cal does not maintain the PHI requested, and knows where the information is, the Medi-Cal program must tell the individual where to request access.

Review of Denials by a Licensed Health Care Professional

When Medi-Cal denies access in instances where the denial is reviewable, and an individual requests review of the decision, Medi-Cal must:

- Designate a health care professional to act as a reviewing official in the case. The reviewing official cannot be someone who participated in the original denial decision;
- Promptly refer the individual's request for review to the designated reviewing official;
- Ensure that the designated reviewing official issues a decision within a reasonable period of time to uphold or overturn the denial;
- Promptly notify the individual, in writing, of the reviewing official's decision; and

- Act according to the reviewing official's decision in providing or denying access to information.

Fees Charged for Access

If an individual requests a copy of the PHI or agrees to a summary or explanation of such information, Medi-Cal may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

- Copying, including the cost of supplies for and labor of copying, the PHI requested by the individual;
- Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
- Preparing an explanation or summary of the PHI, if agreed to by the individual.

No charges, other than postage, should be levied for individuals who wish to inspect a copy of their records and are mailed records, because there is no convenient location for inspection.

Medi-Cal Records Available for Access

Records Held	Responsible for gathering records when access requests are received
Claim Detail Report (CDR) Information up to 10 years old.	EDS has 3 years of current and 3 years of aged CDR data readily available. For the additional 4 years of back data Provider Change Management Branch will need to request an ad hoc report be run to restore this data for printing.
CDR Information dating back beyond 10 years from the current date.	Retained by TPL in microfiche and/or cold storage.
Treatment Authorization Requests (TAR) and Case Management Records.	Held by Medi-Cal Operations Division.
Managed Care records including premium payments, enrollment and disenrollment records, and complaint investigation files.	Held by the Medi-Cal Managed Care Division. Note that individual medical records are maintained by the various managed care plans.

Telephone Request for Access

Telephone requests for access to PHI may be received from:

- The individual;
- Personal Representative;
- Family and/or friends of individual;
- Advocate Groups;
- Medi-Cal Providers;
- Victims of Crimes;
- Dept. of Justice or Dept. of Alcohol and Drug
- Legal Aide;
- Welfare Departments;
- Social Security Administration;
- Legislative Staff;
- Centers for Medicare and Medicaid Services;
- Other State Medicaid Agencies; and
- Health Insurances Plans.

Individual Beneficiary

If the beneficiary calls directly for PHI regarding his or her use, ask for information on the Beneficiary Identification Card (BIC), Social Security Number (SSN), date of birth, phone number and MEDS address to verify identity. If the caller is a representative of the beneficiary, Medi-Cal must verify a personal representative's authority in giving out information about Medi-Cal beneficiaries.

Verification of authority may be difficult to obtain over the phone. The decision to disclose PHI over the phone will be made by the supervisor based on his or her own judgment and past experience.

Legal Basis of Disclosures

Under the Privacy Rule, Medi-Cal may disclose PHI to a family member, other relative or a close personal friend of the Medi-Cal beneficiary or any other person identified by the beneficiary, where PHI is directly related to the person's involvement with

the beneficiary's care or payment. If the Medi-Cal beneficiary is available, Medi-Cal must first obtain the beneficiary's consent before disclosing information or reasonably infer from the circumstances that the beneficiary does not object. In an emergency situation or where the beneficiary is incapacitated or not available, the supervisor may use professional judgment to determine whether the disclosure is in the best interests of the beneficiary. If it is, Medi-Cal may disclose only the PHI directly related to the person's involvement with the individual's health care. (45 CFR 2 §164.510 (b))

The IPA allows personal information to be disclosed with the prior written consent of the individual, to the duly appointed guardian or conservator of the individual or to a person representing the individual if there is documentation that such person is the authorized representative of the individual, if there are compelling circumstances which affect the health or safety of the individual, or to a legislative staff member where the legislator provides reasonable assurance that he or she is acting on behalf of the individual. (Civil Code §1798.24).

With all these rules in mind, Medi-Cal may disclose PHI in response to telephone requests in the following manner; but only if the disclosure is directly related to the administration of the Medi-Cal program.

Levels of Telephone Requests for Information

Level 1

If there is an emergency, the beneficiary is not available and the beneficiary needs immediate care, or is facing other emergent situations causing severe financial or emotional consequences:

- Action – Identify the individual to the best of your ability and find out the relation of the individual to the beneficiary and why the information is needed.
- Result – Consult with your supervisor, then provide the minimum necessary amount of information needed to provide emergency care or help resolve the severe financial or emotional situation.

Level 2

If the situation is critical but there is enough time to receive proper authorization:

- Action – Require a completed Authorization Form from the beneficiary before disclosing information.
- Result – Provide the minimum necessary amount of information requested once the authorization form is received.

Level 3

Information is needed and there is time to receive all required documentation:

- Action – Require a completed Authorization Form and proof of legal relationship such as parent, conservator, executor, legislator acting on behalf of the beneficiary.
- Result – Provide the minimum necessary amount of information requested.

Responding to Beneficiary Calls for Access to Records

When answering calls regarding beneficiary or personal representative requests for access, ask if the beneficiary is enrolled in a managed care plan, and, if so, explain that he/she may need to contact the managed care plan for access to medical records. If the beneficiary needs assistance in calling his/her managed care plan, he or she should be referred to (888) 452-8609.

Also ask the caller if the access request is regarding a personal injury, estate recovery, or worker's compensation case. If the answer is "yes," the caller should be referred to the Third Party Liability Branch at (916) 650-0490.

Forms to be Sent

Requests received by EDS or the Privacy Office for access to Medi-Cal beneficiary records will be responded to by mailing either the Request for Access to PHI Form (DHS 6236) for an Individual or the Request to Access PHI by Parent, Guardian or Personal Representative Form (DHS 6237) for someone other than the individual. These forms include the EDS return address and an EDS contact phone number.

Third Party Liability Requests

If the request for access is in regard to a pending case for estate recovery, personal injury, or workers' compensation, the beneficiary or personal representative should be referred to the Third Party Liability (TPL) Branch at (916) 650-0490.

Requests from Attorneys

If a request is made by an attorney through subpoena or other means for the amount of money which Medi-Cal has paid for services in connection with a personal injury, estate recovery, or worker's compensation claim, a request for access form does not need to be filled out. These disclosures are considered to be directly connected with the operations of the Medi-Cal program. The requestor should be referred to the TPL. If the requestor wants the complete CDR, then the beneficiary has to fill out and sign the request for access form.

Receipt of Request for Access

Upon receipt of the access request form, EDS will verify that the requestor has sent in appropriate identification and payment. If the correct information and/or payment are not included, EDS will send the incomplete form letter, within 3 business days, requesting additional information and/or payment. Checks should be copied and then forwarded to DHS Accounting when all required information is submitted and complete.

The beneficiary may indicate that he/she would like his/her records sent to a person of his/her choosing by marking the appropriate box on page 2 of the form and including the name, telephone number, address, and relationship of the person to the beneficiary. The records can then be sent directly to the person indicated, including an attorney.

If there is any question about the adequacy of the information received from the beneficiary or personal representative, the issue should be referred to the EDS Privacy Officer who should determine if the information received meets the minimum requirements for access.

Minimum requirements include verification of identity and address, and payment as indicated on the form. For personal representatives minimum requirements would include verification of the individual's authority to represent the

individual, such as proof of status as parent or legal guardian, conservator, administrator of the estate, etc. If the information received is equivalent to the requirements of the form, access should be provided. The goal is to provide access without barriers once Medi-Cal is reasonably sure that the person has a right to access the Medi-Cal records.

Fee-for-Service vs. Managed Care

Upon receipt of the access request form, EDS will check the FAME file to see if the beneficiary is enrolled in a managed care plan. If so, EDS will call the beneficiary to ask if there is any reason that DHS may have fee-for-service (FFS) claim information on file. If the beneficiary is enrolled in managed care and no information exists within DHS, the check and form should be returned to the beneficiary.

However, the Medi-Cal Managed Care Division (MMCD) may have some information if the beneficiary has complained about a plan coverage decision. Also, DHS has information on capitation payments made to the plan on the beneficiary's behalf. Ask the beneficiary if he or she wants these records before returning the check.

Request for CDR Information Only

If the requestor asks for CDR information only, EDS will process the CDR and mail it within 15 business days to the requestor. If older information is requested in addition to current information, the beneficiary will be sent a note with the current information explaining that additional information will be coming. For information dating back an additional 3 years, EDS will mail out the information within 30 days of the original request.

If the requestor asks for records dating beyond the 3 year current and 3 year aged records, EDS will immediately notify PCMB and the Privacy Office and an FI letter will be prepared instructing EDS to run CDR information for the remaining 4-year period. In addition, a note will be included with the earlier CDR data to indicate when these records will be provided.

If the requestor asks for CDR information dating back beyond a 10-year period, EDS will contact the Privacy Office, which will gather the information from TPL and send this information directly to the beneficiary.

Request for CDR and TAR or Case Management Records

If the requestor asks for CDR information and either TAR or Case Management records, or both, EDS will send a copy of the request to MCOD within 3 business days of receipt, at the following address:

California Department of Health Services
Medi-Cal Operations Division
Northern Field Operations Branch
PO Box 997419, Mail Stop 4507
Sacramento, CA 94234-7320

(916) 552-9179

EDS will then process the CDR information and send the information along with a cover letter explaining that the MCOD will send the TAR and/or Case Management records to the beneficiary. CDR information will be sent within 15 business days.

Request for TAR and/or Case Management With No CDR

If no CDR information is requested, EDS will send a copy of the request to MCOD at the above address and send a cover letter to the requestor, within 3 business days, explaining that the request has been forwarded to MCOD, providing the requestor with the phone number for MCOD, which is (916) 552-9179.

Subpoena to the Medi-Cal Operations Division

When the MCOD receives a subpoena for records, MCOD will inquire whether the request is directly related to the operation of the Medi-Cal program. If the request is in connection with estate recovery, personal injury, or workers' compensation, the requestor should be referred to TPL at (916) 650-0490.

If the request is for personal purposes, such as a lawsuit not connected to Medi-Cal Operations, MCOD should send the denial letter along with either the Request for Access to Protected Health Information form (DHS 6236) for an Individual or the Request to Access Protected Health Information by Parent, Guardian or Personal Representative Form (DHS 6237) for someone other than the individual. These forms will include the MCOD return address and phone number. The cover letter will include information about the fees for access, stating that

fees must be paid before the request for access will be processed.

MCOD may also want to call attention to the fact that the beneficiary may indicate that he/she would like his/her records sent to a person of his/her choosing, such as the attorney, by marking the appropriate box on page 2 of the form and including the name, telephone number, address, and relationship of the person to the beneficiary. The records can then be sent directly to the person indicated, who may be the beneficiary's attorney or opposing counsel.

Upon receipt of the access request form, MCODE will verify that the requestor has sent in appropriate identification and payment. If the correct information and/or payment are not included, MCODE will send an incomplete form letter, within 3 business days, requesting additional information or payment.

Requests for CDR, TAR and/or Case Management Records

MCOD will process all information requested (CDR, TAR and/or Case Management records) and send all requested information to the requestor. This will eliminate any delay resulting from coordinating the CDR creation with EDS.

MCOD will also determine whether the request for access is related to a third party liability case (Estate Recovery, Personal Injury, or Workers' Compensation) and refer such cases to TPL at (916) 650-0490.

Definitions



Authorization

Authorization is a written instrument whereby a patient or beneficiary consents to the disclosure of PHI about him or her held by a covered health plan or provider to an outside entity designated by the patient or beneficiary.

Designated Record Set

Designated Record Set (DRS) is the group of records maintained by or for a health plan or provider that includes medical and billing records. Specifically, the DRS includes information regarding enrollment, payment, claims adjudication, and case or medical management records systems of Medi-Cal.

Individual

Individual is defined as the person who is the subject of the PHI.

Personal representative

If under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, Medi-Cal must treat such a person as a personal representative with respect to the individual's PHI. Such personal representatives will be treated like the individual with regard to access to the relevant information.

Protected Health Information

Protected health information (PHI) is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Request for Access to PHI (DHS 6236)

Replace with the actual printout of the form.

Request to Access PHI by Parent, Guardian or Personal Representative (DHS 6237)

Replace with the actual printout of the form.

Authorization for Release of PHI (DHS 6247)

Replace with the actual printout of the form.



3 Safeguards

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR §164.530 (c)

Department of Health Services State Administrative Manual

Department of Health Services Information Security Policy

Information Practices Act (IPA): Civil Code §1798.21

Overview

The HIPAA Privacy Rule requires the Department of Health Services (DHS) to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI).

- From any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements related to HIPAA, and
- Reasonably limit incidental uses or disclosures of PHI made inadvertently as a consequence of an otherwise permitted or required use or disclosure.

Administrative safeguards include training, instructions to employees, and documented policies and procedures regarding privacy.

Technical safeguards include computer passwords, timing out of screens, laptop security and encryption.

Physical safeguards include locks on file cabinets, door locks, partitions, shredders, and confidential destruct.

MAJOR CONSIDERATION: IPA and safeguards

State agencies that are covered entities are able to comply with both the HIPAA safeguard requirements and the IPA safeguard requirements, and, therefore, State agencies **must comply with both rules.**

The IPA is similar to HIPAA but is more stringent by including requirements to protect records against anticipated threats or hazards to the security or integrity that could result in any injury.

The Safeguards Section includes:

- Information Security Policy
- Health Administrative Manual
- Administrative Safeguards
 - Training
 - Instructions to Employees
 - Policies and Procedures
- Technical Safeguards
 - Computer Passwords
 - Computer Monitors
 - Computer Peripherals
 - Laptop Computers
- Physical Safeguards
 - Paper Files
 - Faxes
 - Mail
 - Oral Communications

Policy



It is the policy of the Medi-Cal program to take reasonable steps to safeguard confidential information/PHI from any intentional or unintentional use or disclosure that is in violation of the privacy policies and to establish new policies to safeguard PHI. PHI may be in any medium, including paper, electronic, oral, and visual representations of confidential information. Medi-Cal should conduct internal reviews periodically to evaluate current safeguards. DHS policies are found in Section 6100 *Information Security Policy of the Health Administrative Manual (HAM)*.

Information Security Policy

Medi-Cal should provide appropriate protection from loss, inappropriate disclosure, and unauthorized modification of automated files and databases. This protection includes, but is not limited to, strict controls to prevent unauthorized access to data maintained in computer files, program documentation, data processing systems, data files, and data processing equipment physically located in the department. Employees are responsible for the security of their computer and their data. Employees are responsible for the confidentiality and security of their passwords. In performing Medi-Cal business, the employee should take every precaution to ensure the security of the information. Confidential information, including PHI, may be transmitted via Internet and/or E-mail only when the following conditions have been met:

1. Program management approvals have been obtained; *and*
2. Encryption, authentication, and/or any other Medi-Cal Information Security Officer (ISO) approved security schemes and/or policies are used to ensure that data is secured and made available to the appropriate and intended recipients only. (State Administrative Manual (SAM) §§4840-4845.)

The SAM §4842.2 under Personnel Practices requires that all employees receive training on DHS information security policies, and sign acknowledgments of their security responsibility. Each employee is provided a copy of the Information Security Policy agreeing to comply with the security requirements indicated in the policy.

DHS has designated an ISO staff member who should be responsible for implementing state policies and standards regarding the confidentiality and security of information.

To reach the ISO, email:

SECADMIN@dhs.ca.gov

The ISO website is:

[http://itsd.int.dhs.ca.gov/4 information security/](http://itsd.int.dhs.ca.gov/4%20information%20security/)

Health Administrative Manual (HAM)

Access to Department Records – HAM Policy 11-3030

Employees are required to maintain record and equipment security measures that preserve privacy and prevent the loss of confidential information through accident, sabotage, or natural disaster.

Security of Confidential Information – HAM Policy 11-3060

Programs must provide adequate protection for all office facilities and equipment that contain confidential information. Security procedures should strike a balance between the risk of a breach of security and the staff's need to work with the information.

During normal work hours, confidential information may not be left unattended. If the area will be unattended, even for only a few minutes, confidential information, including PHI, must be locked up. Program staff must escort visitors, and confidential information, including PHI, should be kept out of sight while they are in the area.

During nonworking hours confidential information, including PHI, must be kept in a locked desk or cabinet, even if the building is secured.

Once confidential information, including PHI, has met its designated retention period, it must be disposed of through confidential means (shredded, pulverized, etc.) and disposal must be witnessed by a state employee. See HAM, section 11-2060 and contact Records Management and Administrative Support (RMAS) for assistance if you have any questions.

Procedures



The following procedures should be used to ensure that all Medi-Cal employees safeguard PHI.

Administrative Safeguards

Administrative safeguards are administrative actions, and policies and procedures to:

- Manage the selection, development, implementation, and maintenance of security measures to protect PHI, and
- Manage the conduct of the covered entity's workforce in relation to the protection of that information.

Administrative safeguards include training, instructions to employees, and policies and procedures regarding privacy.

Medi-Cal will provide/conduct:

- Training to all staff (including trainees, contractors, students, and interns, paid and volunteer, who perform services for Medi-Cal) on the privacy policies and procedures with respect to PHI, as necessary and appropriate for members of the workforce to carry out their functions for Medi-Cal.
- Training to staff regarding each employee's role in protecting PHI.
- Internal reviews periodically in order to evaluate the effectiveness of current safeguards.

Technical Safeguards

Technical safeguards are the technology, the policy, and the procedures that protect electronic PHI and control access to it. Technical safeguards include computer passwords, monitors, laptop security and encryption.

Computer Passwords

Medi-Cal staff will:

- Not share passwords;
- Select an unusual combination of a minimum of 8 characters or more for a secure password;
- Keep passwords confidential, including passwords used for dial-up access. They are not to be written down, posted where they may be accessed, or included in a data file, log-on script, or macro. Example: macros to connect to MEDS;
- Change their passwords immediately if revealed or compromised or suspected to be revealed or compromised;
- Change their passwords every 60 days; and
- Report any suspected unauthorized use of an ID or password to their supervisor and the Medi-Cal ISO immediately.

Computer Monitors

Medi-Cal staff will:

- Use a timed screen saver requiring passwords for access, so that accessed information will continue to be protected while logged-on. Upon leaving their desks, all staff will use Control Alt Delete to lock their computer.
- Ensure that observable PHI is adequately shielded from unauthorized disclosure on computer screens. To avoid unintentional access to an individual's PHI, turn the monitor in a direction away from public access whether in a reception area or workstation (cubicle).

Computers Peripherals

Medi-Cal staff will:

- Place removable media, e.g., CD's and disks, in an enclosed or locked area when not in use.
- Not store confidential or critical data on a personal computer (PC) unless adequate security precautions have been taken.

- Not send e-mail messages containing PHI to groups outside of DHS such as Dept. of Justice or Dept. of Social Services, as the communication links are not secure. Use fax, courier or overnight mail to transfer PHI to outside departments.
- Only send the minimum necessary amount of PHI via email within DHS.
- Include policy statement on the bottom of email (OUTLOOK) below your signature block. To add this to your current signature:
 - a. Open new message. Automatic signature block must be in a blank message.
 - b. Type Privacy message below your original signature block.
 - c. Highlight your message.
 - d. Click “tools” in the menu bar.
 - e. Select Auto Signature.

Example of statement is:

The information contained on the Email document is confidential and intended only to be viewed by the recipient listed above. If you are not the intended recipient (or the employee or agent responsible to deliver this to the intended recipient), you are hereby notified that any distribution or copying of this document is strictly prohibited. If you have received this document in error, please contact the sender listed above and destroy the document.

Laptop Computers

Take extra caution while working with PHI on a laptop computer, **always** logging off, and placing in a secure location. Staff should use locking briefcases as provided by the DHS. Laptops containing PHI should not be separated from staff-not at airports, in automobiles, or hotel rooms. Theft and loss of laptops is one of the highest risks for security breaches. Avoid downloading PHI to laptops unless all data is encrypted.

Medi-Cal staff will:

- Take extra caution while working with PHI on a laptop computer, logging off, and placing in a secure location.

- Not store confidential or critical data on a laptop unless adequate security precautions have been taken.
- Not leave laptop unattended at workplace, home, or in vehicle.
- Lock the laptop in a drawer, cabinet, or secure in a location that is not visible.
- Not share any passwords, including encryption passwords.
- Place removable media, e.g., CD's and disks, which contains PHI in a secure area when not in use.
- Use caution when sending e-mail or transporting documents within the DHS network to ensure that the recipient knows that sensitive information is being exchanged.
- Follow the DHS Mobile Computing Policy in the HAM (See Appendix).

Physical Safeguards

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Physical safeguards include security of paper files (including fax and mail), locks on file cabinets, door locks, partitions, shredders, and oral communication.

Paper Files

Medi-Cal staff will:

- Store files and documents in locked file cabinets. Cabinets, if necessary, may be stored in a locked/secured room or storage system.
- Keep PHI locked in a desk or cabinet during nonworking hours, even if the building is secured.
- Make every effort to take reasonable steps to ensure the safeguarding of PHI if locked cabinets are not available. Turning documents with PHI face down on worktops, placing documents in a drawer, or even keeping documents in a folder can accomplish this.

- Limit staff access to secured files to alleviate unnecessary access to files. Files should be used on a “need to know” basis.
- Provide containers specifically for the destruction of confidential (PHI) information. Each container will be clearly identified as “Confidential”.
- Dispose of PHI through confidential means (shredded, pulverized, etc.) once confidential information has met its designated retention period. A state employee must witness disposal.

Removing Records from a DHS Facility

Employees like those in MCOB, who take records containing PHI into the field, should safeguard those records by taking the following steps:

- Staff must ensure that all records containing PHI are "inventoried", either by way of MCM's tracking system or UR's "keying" in treatment authorization requests (TARs) and assigning a document control number.
- In no case may employees keep records containing PHI in their possession beyond the time when such custody of the records is absolutely necessary for performing their job functions. Staff must return all such records to their DHS offices when the records containing PHI are no longer needed for their job functions.
- Staff are not to discard PHI on their own, and must return all PHI to their DHS offices for confidential destruction. Do not store medical records in homes or private storage units.
- If a field office is closed or moved, staff should be assigned specific duties during a closure or move to ensure confidentiality is maintained.

Faxes

Medi-Cal staff will:

- Be assigned to regularly check for faxes, place the fax in a manila folder to protect any PHI, and deliver to the addressee in a timely manner.

- Place fax machines that receive or transmit PHI, away from potential access by the public.
- When sending faxes, notify the recipient that a document is being faxed, verifying the fax number at the time.
- Not leave faxes unattended if not in a secure area.
- Have a designated fax machine for receiving and sending highly confidential faxes.
- Add a confidentiality statement at the beginning or at the end of every fax that contains PHI. Medi-Cal staff may use the confidentiality statement recommended by the Privacy Office:

“The information contained on the faxed document is confidential and intended only to be viewed by the recipient listed above. If you are not the intended recipient (or the employee or agent responsible to deliver this to the intended recipient), you are hereby notified that any distribution or copying of this document is strictly prohibited. If you have received this document in error, please contact the sender listed above and destroy the document.”

Mail

Medi-Cal staff will:

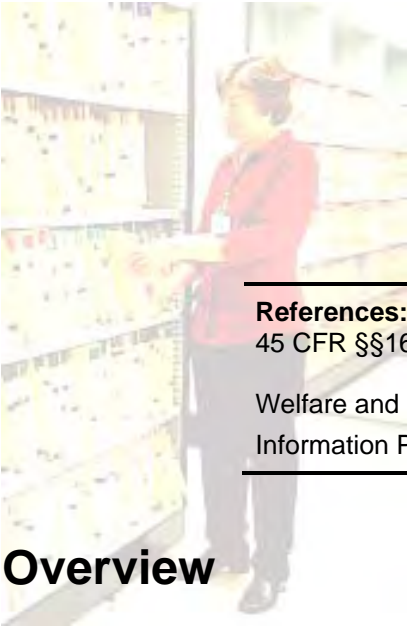
- Verify the address prior to sending correspondences that contain PHI
- Ensure that the address on the envelope has been accurately transcribed. Assure that outgoing correspondences that contain PHI, especially a Social Security Number (SSN), are placed in an envelope so this information is not visible.
- Use encryption software for disks when disks that contain PHI are sent through the mail. United States Postal Service mail is considered to be a secure method of delivery, but if a large quantity of PHI needs to be mailed, it should be on an encrypted disk or CD and sent by a secure courier, such as Federal Express.
- Assure that incoming correspondences that are marked confidential are delivered unopened to the intended recipient.

- Regularly update directories and related client databases with current contact information.

Oral Communications

Medi-Cal staff will:

- Take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs (telephone, restrooms, break rooms, etc.)
- Find enclosed offices and/or interview rooms for the verbal exchange of confidential information.
- Promote employee awareness of the potential for inadvertent verbal disclosure of confidential information.
- Verify the identity of the person to whom you are verbally exchanging PHI.
- Ask for the information on the individual's benefits identification card (BIC).
- If individuals don't have a BIC, ask for their SSN, date of birth, phone number, and address on MEDS (enough information so you are satisfied that they are whom they say they are).
- Ensure the verbal exchange is an authorized disclosure.



4 Uses and Disclosures

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR §§164.502; 164.504; 164.506; 164.512; 164.514

Welfare and Institutions Code §14100.2; 42 CFR 431.300 *et seq.*
Information Practices Act (IPA) – Civil Code §1798.24

Overview

The Privacy Rule lays out the permissible uses and disclosures of protected health information (PHI), which health plans and providers covered by HIPAA are allowed to make.

Under the law, HIPAA covered entities such as Medi-Cal must disclose PHI:

- To an individual, when requested under and required by the HIPAA rules, specifically the rules that grant individuals the right to inspect and obtain a copy of their PHI and to obtain an accounting of the use and disclosure of their PHI.
- To the Secretary of the U.S. Department of Health and Human Services (DHHS), under his/her authority in the HIPAA Privacy Rule to require disclosure to investigate and determine the covered entity's compliance with HIPAA rules related to privacy.

Almost all Department of Health Services (DHS) covered health plan/provider programs have controlling federal and state statutes which restrict uses and disclosures to purposes connected with the administration of those programs or other purposes, such as research, specifically described by statute. DHS programs must follow these more restrictive statutes and regulations in using and disclosing PHI in their possession, since HIPAA does not preempt these more restrictive privacy statutes.

For the Medi-Cal program, uses and disclosures are primarily controlled by federal regulations and implementing State statute.

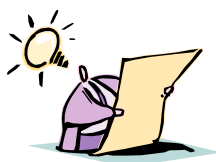
Federal regulations require that State Medicaid programs, such as Medi-Cal, “restrict the use or disclosure of information

concerning applicants and recipients to purposes directly connected with the administration of the [Medicaid] plan.” 42 Code of Federal Regulations §431.300. California Welfare and Institutions Code §14100.2 mandates that all types of information, whether written or oral, concerning a person made or kept by any public agency in connection with the Medi-Cal program should be confidential and should only be used or disclosed “for purposes directly connected with the administration of the Medi-Cal program.” Such information includes but is not limited to, names and addresses, medical services provided, social and economic conditions, medical data, etc. Purposes directly connected with administration of the Medi-Cal program include program operations, such as establishing eligibility and methods of reimbursement; providing services; conducting investigations or prosecutions related to Medi-Cal, etc.

The Uses and Disclosures of PHI section includes:

- Uses and Disclosures for the Medi-Cal Program;
- Definition of Use and Disclosure;
- Disclosures for Limited Purposes;
- Authorizations for Uses and Disclosures;
- Uses and Disclosures for Treatment, Payment and Operations;
- Uses and Disclosures to Business Associates;
- Minimum Necessary PHI to be Used and Disclosed;
- Uses and Disclosures to Health Oversight Agencies;
- Uses and Disclosures in Judicial Proceedings; and
- Definitions.

Policy



The policy of the Medi-Cal program is to only use and disclose PHI in accordance with all applicable state and federal laws. Specifically, Medi-Cal PHI may only be used or disclosed for purposes directly connected with the administration of the Medi-Cal program.

Uses and Disclosures for the Medi-Cal Program

Federal and State laws on disclosure of information by the Medi-Cal program are very strict. The law requires that all types of information, whether written or oral, concerning a person made or kept by any public officer or agency in connection with Medicaid should be confidential and should only be used and disclosed for purposes directly connected with the administration of the Medi-Cal program.

Thus, the uses and disclosures of PHI under Medi-Cal are limited to purposes directly connected with the administration of Medi-Cal, which is defined as those administrative activities which DHS and its agents are required to engage in to ensure effective program operations, including, but not limited to:

- Establishing eligibility and methods of reimbursement;
- Determining the amount of medical assistance;
- Providing services for recipients;
- Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of Medi-Cal;
- Third party recovery activities; and
- Conducting or assisting a legislative investigation or audit related to the administration of Medi-Cal.

Definition of Use and Disclosure

Use applies to covered entities; for members of the covered entities' workforce and the business associates' workforce to use or disclose PHI to accomplish their purposes. Minimum necessary applies to all uses except for treatment.

Disclosure applies to anyone else; for persons or organizations who receive PHI from covered entities or the covered entities' business associates. Minimum necessary applies to most disclosures. When the Medi-Cal program shares data with another DHS program, such as public health, that is considered a disclosure.

Disclosures for Limited Purposes

HIPAA permits covered entities to use or disclose PHI for limited purposes. [45 C.F.R. §164.506] These limited purposes include:

- Authorizations;
- Treatment, Payment and Health Care Operations;
(Only health care providers are allowed to use PHI for treatment purposes, because only providers conduct treatment).
- Required Disclosures;
(To the Individual, to the Secretary of U.S. DHHS)
- Health Oversight;
(Audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions.)
- Public Policy.
(Activities required by law, public health activities, health oversight activities, judicial or administrative proceedings, law enforcement, deceased individuals, organ donations, research with institutional review boards/policy board approval or data use agreements, health and safety, specific government functions, victims of abuse, neglect, or domestic violence, or workers' compensation.)

Please note that Medi-Cal may make such disclosures only if directly connected with the administration of the Medi-Cal program.

Authorizations for Use and Disclosure

HIPAA allows a covered entity to use or disclose PHI with an authorization from the individual. An authorization must be used for disclosure of:

- Psychotherapy notes
- Marketing activities

And in all circumstances where:

- HIPAA does not permit use or disclosure;
- The covered entity has determined that an authorization is required as part of their Privacy Policies and Procedure; and
- An authorization is required by law.

Please note that Medi-Cal may not disclose PHI even with a beneficiary authorization if the purpose for the release is not directly connected with administration of the Medi-Cal program. In case of lawsuits where DHS is not a party and where the beneficiary is suing for personal injury or workers' compensation, for example, PHI may only be released by a court order or by a properly executed request for access form signed by the Medi-Cal beneficiary. (DHS form 6236)

Use and Disclosure for Treatment, Payment, and Operations (TPO)

In general, HIPAA covered providers are allowed to use and disclose PHI for treatment and health plans such as Medi-Cal are allowed to use and disclose PHI for payment activities and their own operations, without obtaining an authorization from a program beneficiary or patient. Of course, these uses and disclosures must otherwise comply with the Privacy Rule and with other state and federal statutes on confidentiality of information pertaining to the Medi-Cal program.

The rule for disclosing information for payment purposes is that the HIPAA covered health plan may only disclose PHI to another covered entity (e.g. health plan or clearinghouse) or a health care provider for the payment activities of the entity that receives the PHI.

For health operations, the HIPAA rule is that a covered health plan or provider may only disclose PHI to another covered entity for certain health care operations activities of the entity that receives the information, if each entity has or had a relationship with the same patient who is the subject of the PHI being requested and the PHI pertains to that relationship.

The health care operations activities which allow this sharing include: health care fraud and abuse detection, compliance, conducting quality assurance, case management and care coordination, improving health or reducing health care costs, contacting patients and providers with information about

treatment alternatives, reviewing competence or qualifications of health care professionals, evaluating provider or health plan performance, training, accreditation, certification, licensing, or credentialing. An example is managed care plans disclosing encounter data to the Medi-Cal program.

Uses and Disclosures to Business Associates

When a covered health plan such as Medi-Cal discloses PHI to a contractor which is doing work on behalf of the health plan involving payment or health plan operations, that disclosure is permitted so long as the contractor has signed a business associate agreement with the covered health plan or provider, which complies with the Privacy Rule (See Guidance on Business Associate Agreements). Business associate language must be included in any contracts entered into, renewed or amended, or in all contracts by April 14, 2004. Some business associates of Medi-Cal are other governmental entities such as Dept. of Social Services, State Controllers' Office, Dept. of Mental Health, Alcohol & Drug Program, and Office of Aging. In this case, Medi-Cal should put language into the contract or Inter-Agency Agreement with the other governmental organization indicating that organization's agreement to be bound by the HIPAA rules and the rules for Medi-Cal uses and disclosures.

The Minimum Necessary PHI to Be Used or Disclosed

When using PHI or when requesting PHI from another covered entity, Medi-Cal will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. (See Policy on Minimum Necessary.)

Uses and Disclosures to Health Oversight Agencies

A health oversight agency is authorized by law to conduct certain oversight activities, including audits, civil, administrative or criminal investigations, proceedings, or actions, inspections, licensure or disciplinary actions, or other activities necessary for appropriate oversight of the health care system, government benefit programs for which health information is relevant to beneficiary eligibility, or entities regulated by the government for which health information is necessary for determining compliance with program standards. (45 CFR §164.512(d)) Medi-Cal may disclose PHI to the Bureau of State Audits, the

Bureau of Medical Quality Assurance, the Department of Justice (DOJ) and the Federal Bureau of Investigations (FBI), for example, as health oversight agencies so long as the disclosures are directly connected with the administration of the Medi-Cal program.

Uses and Disclosures in Judicial Proceedings

According to the federal Office for Civil Rights, when a health plan such as Medi-Cal, is a party to a legal proceeding, Medi-Cal may use or disclose PHI for purposes of litigation as part of its health care operations. Medi-Cal must limit such uses and disclosures to the minimum necessary to accomplish the intended purpose. Medi-Cal attorneys who are DHS employees must make reasonable efforts to limit the PHI disclosed to the minimum necessary for the purpose of the disclosure.

When Medi-Cal is not a party to litigation, if the litigation is not directly connected to the administration of the Medi-Cal program, neither Medi-Cal nor its lawyers may disclose PHI in response to a subpoena or other request. A court order and prior notification of the beneficiary is required. In the case of Medi-Cal fraud criminal prosecutions, disclosures of PHI may be considered allowable disclosures to health oversight agencies, such as the FBI or the DOJ and do not require subpoenas.

Procedures



The following procedures are to be followed in connection with Medi-Cal Uses and Disclosures.

DHS employees are not to disclose Medi-Cal PHI under any circumstances where the disclosure is not directly connected to the administration of Medi-Cal. If a DHS employee receives a subpoena for Medi-Cal records, the employee should contact Medi-Cal house counsel. If a DHS unit receives a request for records containing Medi-Cal PHI, and there is a question about the legality of release of the records, the employee should contact the DHS Privacy Officer.

Definitions



Authorization

Authorization is a written instrument whereby a patient or beneficiary consents to the disclosure of PHI about him or her held by a covered health plan or provider to an outside entity designated by the patient or beneficiary.

Covered entities

Covered entities are health plans, health care clearinghouses, and health care providers who conduct any standard electronic transactions.

Disclosure

Disclosure is the release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

Operations

Operations is conducting quality assessment and improvement activities, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; evaluating practitioner and provider performance, health plan performance, certification or credentialing activities; conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; formulary development and administration; development or improvement of methods of payment or coverage policies; and business management and general administrative activities of the entity.

Payment

Payment is activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or activities by a health care provider or health plan to obtain or provide reimbursement for the provision of health care. Such activities include determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing) and adjudication of health benefit claims, billing, claims management, collection activities, health care data processing, review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or

justification of charges, utilization review activities including prior authorization of services.

Protected Health Information (PHI)

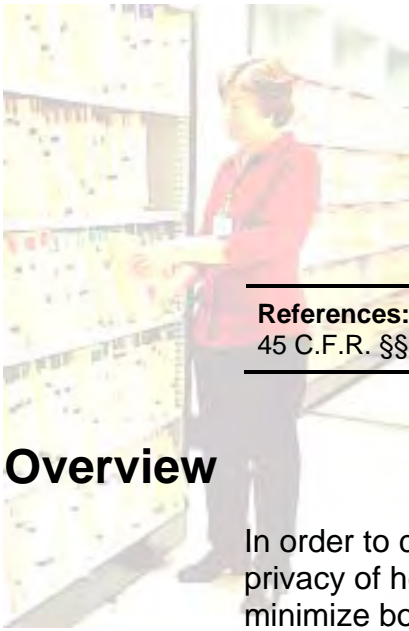
PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Treatment

Treatment is the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use

Use is the sharing, application, utilization, examination, or analysis of PHI within a covered health plan or provider which maintains the information.



5 Minimum Necessary

References: Health Insurance Portability and Accountability Act (HIPAA)
45 C.F.R. §§164.502(b)(1), 164.514 (d)

Overview

In order to comply with state and federal laws protecting the privacy of health information, the Medi-Cal program must minimize both the amount of protected health information (PHI) used and disclosed and the number of persons who have access to such information.

When using or disclosing PHI or when requesting PHI from another covered entity, Medi-Cal must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended use, disclosure, or request.

In other words, Minimum Necessary means only accessing and using PHI that is absolutely needed for staff members to perform their job functions.

Medi-Cal units must implement policies and procedures or standard protocols that limit the PHI used or disclosed to the amount reasonably necessary to achieve the purpose for their uses and disclosures.

Medi-Cal must also limit access to systems containing PHI, such as the Medi-Cal Eligibility Data Systems (MEDS), to only those staff whose job descriptions require access to data in the systems.

Medi-Cal is expected to incur reasonable expenses in limiting the use and disclosure of PHI.

Medi-Cal should determine whether de-identified information may be used before applying the minimum necessary rule.

This section explains the Medi-Cal guidelines used to determine the minimum necessary amount of PHI accessed and used by staff members as well as disclosed to entities outside the Medi-Cal program.

The Minimum Necessary section includes:

- Disclosures of PHI;
- Use of PHI within Dept. of Health Services;
- Documentation;
- Program Management Responsibilities; and
- Definitions.

Policy



The policy of Medi-Cal is to meet the minimum necessary requirements in the Privacy Rule. Medi-Cal must implement policies and procedures or standard protocols that limit the PHI used or disclosed to the amount reasonably necessary to achieve the purpose.

Medi-Cal staff must:

- Develop criteria to limit the PHI used or disclosed to the information reasonably necessary to accomplish the purpose for which the disclosure is sought;
- Review requests for disclosure on an individual basis in accordance with such criteria; and
- Allow access to electronic systems containing PHI to only those staff whose jobs require such data.

The minimum necessary standard does not apply to the following situations:

- Disclosures to or requests for information by a health care provider for treatment purposes;
- Disclosures made to the individual;
- Uses or disclosures made pursuant to an authorization from the individual;
- Disclosures to the U.S. Secretary of Health and Human Services;
- Uses or disclosures required by law, and
- Uses or disclosures required for compliance with HIPAA.

Procedures



The following procedures should be used to ensure that all Medi-Cal employees adhere to the minimum necessary rule.

Use of PHI within Department of Health Services

The Medi-Cal program is required to take steps to limit how the staff use, disclose, or request PHI. Medi-Cal is required to identify classes of employees or staff needing access to PHI to carry out their duties, the types of PHI to which they need access, and the methods to limit access.

Please note that programs in Department of Health Services (DHS) outside of Medi-Cal and its internal business associates, i.e. Audits & Investigations, Legal, Accounting, Information Technology Services Division (ITSD), Fiscal Forecasting and Data Management are treated like outside entities for purposes of disclosures of PHI.

The basic standard for minimum necessary uses requires that Medi-Cal make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the program. Therefore, Medi-Cal must develop role-based access policies that allow its employees access to beneficiary information, as appropriate. This may include access to the entire record for specific purposes, if necessary. With electronic information, Medi-Cal should take reasonable steps to configure their record systems to allow access to only certain data fields and for certain purposes.

The fields of information that are disclosed should:

- Remove identifiers (including names, addresses and other data);
- Encrypt restricted information so that only authorized personnel have the ability to link identifiers back to the record;
- Limit review, forwarding, and printing to only those fields and records relevant to the user's need for information;

- Allow selective access to different portions of the record, so that administrative personnel get access to only certain fields, and medical personnel get access to other fields; and
- For electronic systems, such as MEDS, unique identifiers and passwords should be assigned to only those staff whose jobs require access to these systems. These identifiers and passwords should not be shared, and must be terminated when staff change positions or leave the Medi-Cal program.

For non-electronic information, Medi-Cal should adopt the following procedures to meet the minimum necessary requirements:

- The selective copying of relevant parts of PHI, or
- Allow staff to order only those portions of reports they need for their job responsibilities.

Disclosures of PHI

To determine the minimal amount of PHI to disclose, Medi-Cal staff should use the following guidelines:

Public Officials

Medi-Cal staff may rely on the requested disclosure as the minimum necessary for the stated purpose when making disclosures to public officials, given proper identification of the organization and official.

Disclosures to Other Covered Entities

Medi-Cal staff may reasonably rely on the request of another covered entity (health provider, health plan, health care clearinghouse) because the requesting covered entity is itself subject to the minimum necessary standard. Therefore, the requesting covered entity is required to limit its request to only that information that is reasonably necessary for the purpose. However, if Medi-Cal believes that the amount of information requested by another covered entity is not reasonably necessary for the purpose, it is up to Medi-Cal staff to work with the other covered entity to negotiate a resolution of the dispute as to the amount of information needed.

Business Associates

The minimum necessary standard applies to disclosures to business associates. However, the burden on Medi-Cal is lessened in working with business associates. In the business associate contract Medi-Cal must limit the business associate's uses and disclosures of, as well as requests for, PHI to be consistent with the Medi-Cal program's minimum necessary policies and procedures.

Medi-Cal units should develop standard protocols to apply to routine disclosures made to business associates, and individual review of these routine disclosures may be eliminated.

Medi-Cal is allowed to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for the purpose.

Research

Medi-Cal may rely on a researcher's documentation of an IRB or Privacy Board waiver of authorization that the information requested is the minimum necessary for the research purpose. This is true regardless of whether the documentation is obtained from an external IRB or Privacy Board or from one that is associated with the DHS. Medi-Cal may also reasonably rely on a representation made by the requestor that the information is necessary to prepare a research protocol.

Required by Law

DHS may use or disclose PHI as required by law. The minimum necessary standard does not apply to uses and disclosures required by law, but rather the amount of information used or disclosed is limited by the authority granted in the law.

Public Health or Health Oversight/As Required By Law

Due to heightened awareness of privacy issues, Medi-Cal Audits and Investigations and other DHS components may experience a reluctance of covered entities to disclose PHI. DHS programs should be prepared to provide the authority provided in law for the collection of information. The minimum necessary information would then be limited to the information set out in the statutory authority.

Where no statutory authority exists, DHS programs may need to get authorization from the individual in order to get access to PHI. These requests would be limited to the minimum necessary information needed for the stated purpose.

Documentation

HIPAA requires covered entities to document actions, activities, designations and written communications required by the Privacy Rule. These policies and procedures and the specific designation of classes of staff allowed to access systems of PHI fulfill the Privacy Rule for minimum necessary documentation. (See Minimum Necessary chart in the Appendix.)

Program Management Responsibilities

Medi-Cal managers have the following responsibilities in implementing “minimum necessary:

- Develop individual or role-based access procedures for Medi-Cal employees, considering HIPAA policies and procedures and implementing as appropriate for individual employees and work situations;
- Follow the criteria for use of PHI within DHS as specified in the Minimum Necessary Policy, in the MEDS policy, and any other DHS data policy;
- Establish criteria to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which the disclosure is sought;
- Train employees on the procedures that have been established for each work area and employee;
- Adapt the access level of PHI for employees as job functions change;
- Take reasonable steps to configure record systems to allow access to only certain data fields as required by individual employees;
- Teach employees how to use de-identified information, particularly in training and research;
- Educate employees on what can be used/looked at as part of their job responsibility. If an employee has access to a

database, the employee need only look at the portions of data that are relevant to the employee's job duties;

- Assure that non-electronic information meets the minimum necessary requirements, including the selective copying of relevant parts of PHI and limiting the portions of documents available to employees to that which is necessary to perform their job functions;
- Treat PHI on a "need to know" basis. PHI should only be shared with other employees that have a need to know the information in order to perform a job function. Employees should not discuss PHI with employees that do not have a need to know.

Definitions



Covered Entity

Covered entity means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Privacy Rule

The Privacy Rule are regulations implementing the set "Standards for Privacy of Individually Identifiable Health Information", found at 45 CFR Parts 160 and 164.

Individually Identifiable Health Information

Individually identifiable health information is information that identifies the individual or may be used to identify the individual, and contains detailed health information about persons, including such things as address, gender, age and spoken language, etc.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.



6 Request Restriction of Uses or Disclosures of Protected Health Information

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part 164.522

Overview

The HIPAA Privacy Rule states individuals may make a request to a health plan, such as Medi-Cal, to limit how their health information is used and shared with others.

The main uses of health care data are:

- For the treatment of a member;
- For the payment to a provider for health care services; or
- For the operations of the health plan.

The health plan may also need to share this detailed information with someone other than the member of the health plan.

Sharing this data may be needed because someone other than the member is responsible for that member's care. A health plan may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information (PHI) directly related to such person's involvement with the individual's care or payment related to the individual's health care [45 CFR §164.510(b)]. See Individual Access.

The only restrictions on uses and disclosures which an individual may request under HIPAA are to carry out treatment, payment, or health care operations, or to restrict disclosures to persons, such as family members, relatives, and close personal friends involved with the individual's care or payment. Medi-Cal is not required under the Privacy Rule to agree to a restriction.

The Restrictions of Uses and Disclosures Section includes:

- Process to Request Restrictions of Uses and Disclosures of PHI;
- Agreeing to Restriction of Use and Disclosure of PHI;
- Department of Health Services (DHS) is Not Required to Agree with Restriction Request;
- Termination of Restriction of Use and Disclosure of PHI;
- Definitions;
- Request to Restrict Use and Disclosure of PHI (DHS 6240); and
- Request to Restrict Use and Disclosure of PHI by Parent, Guardian or Personal Representative (DHS 6241)

Policy



It is the policy of the Medi-Cal program to allow individuals the right to request the restriction of uses and disclosures of their PHI. Medi-Cal must allow individuals to request that it restrict uses and disclosures of PHI about them to carry out treatment, payment, or health care operations or to those involved with the individual's care or payment. All requests for restriction of uses and disclosures of PHI must be made in writing using the Request to Restrict Use and Disclosure of PHI form (DHS 6240).

Procedures



The following procedures define the process to be used by Medi-Cal staff to respond to requests to restrict uses and disclosures of PHI.

Process to Request Restriction of Uses and Disclosures of PHI

Medi-Cal will provide the Request to Restrict Use and Disclosure of PHI form (DHS 6240) to individuals requesting to restrict uses and disclosures of PHI.

In order to ensure that Medi-Cal is protecting individual health information, individuals requesting to restrict uses and

disclosures of PHI must verify their identities. A photocopy of one of the following must accompany a request for restriction:

- Birth Certificate;
- California Driver's License;
- Beneficiary ID Card;
- Managed Care Card; or
- State or Federal Employee ID Card.

A notarized signature can be provided in lieu of a copy of one of the listed identifiers. Information will only be sent to the address listed for the individual in the Medi-Cal file. If individuals wish to change their address, they must contact the county welfare department for an address change before requesting that information be sent to that address.

Upon receipt of request for restriction of PHI, Medi-Cal staff will review and determine if the request will be granted or denied in a timely manner.

Medi-Cal staff will respond in writing to the individual with a decision, including a copy of the request, and the reasons for granting or denying the request.

Upon agreement to the restriction, DHS staff will not use or disclose information that violates the restriction.

Prior to any use or disclosure of an individual's PHI, Medi-Cal staff will confirm that such use or disclosure has not been restricted, by reviewing its records.

DHS will retain all documentation relating to requests for restrictions on use and/or disclosure of individuals' PHI for a minimum of six years.

Agreeing to Restriction of Use and Disclosures of PHI

If Medi-Cal agrees to a restriction, it cannot use or share the individual's PHI in any way that violates that restriction except in situations when the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the treatment.

If the restricted PHI is disclosed to a health care provider for emergency treatment, as described above, Medi-Cal must

request that the health care provider no longer use or disclose the information.

An agreement to restrict is not effective to prevent uses or disclosures of PHI that are required: by the Secretary (Health and Human Services) to investigate or determine compliance by DHS; for facility directories; by law; for public health activities; about victims of abuse, neglect, or domestic violence; for judicial and administrative proceedings; for law enforcement purposes; about decedents; for cadaveric organ, eye, or tissue donation purposes; for research purposes; to avert serious threat to health or safety; for specialized government functions; or for workers' compensation.

DHS is Not Required to Agree With the Restriction Requested By an Individual

Medi-Cal is not required to agree to a restriction.

Nothing in the HIPAA Privacy Rule requires a health plan to agree to a request to restrict, or to treat or provide coverage to an individual requesting a restriction under the rule.

Medi-Cal would not be bound by an individual's request for restriction until its scope has been agreed to by the individual and the program. Once the agreement has been reached, use or disclosure of PHI that violates such agreement would be in violation of the HIPAA Privacy Rule.

Termination of Restriction of Use and Disclosure of PHI

An agreement to a restriction may be terminated by the individual or Medi-Cal.

The request for termination of the agreement must be made in writing. The request can be made orally if the oral agreement is documented.

Medi-Cal must apply its policy of termination of an agreement consistently among individuals.

The agreement to a restriction must be documented and must be retained for six years from the date it was created or the date it was last in effect, whichever is later.

If the individual terminates the agreement to a restriction, the request for termination must be in writing. DHS will place the request in its files to terminate the restriction.

Medi-Cal may terminate its agreement to restrict by informing the individual in writing. Information that was created or received while the restriction was in effect will remain subject to the restriction.

Definitions



Health care operations

Health care operations mean any activities of a health plan that are related to its operations.

Examples of health care operations activities are:

- Conducting quality assessment and improvement activities;
- Reviewing the competence or qualifications of health care professionals;
- Underwriting and/or premium rating;
- Conducting or arranging for medical review;
- Legal services;
- Business planning and development;
- Business management and general administrative activities such as claims payment;
- Customer service; and
- Resolution of internal grievances.

Payment

Payment means the activities performed by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Activities performed to obtain payment include:

- Determining the eligibility or coverage of an individual;
- Coordinating the benefits or cost sharing amounts of an individual;

- Reviewing and adjusting provider contract or premium amounts based on the health status and demographic characteristics of their members;
- Premium billing and collection activities;
- Claims management and adjudication. Obtaining payment under a contract for reinsurance including stop-loss insurance and excess of loss insurance;
- Reviewing health care services with respect to medical necessity, coverage under the health plan, appropriateness of care, or justification of charges; and
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

Privacy Rule

The Privacy Rule is regulations implementing the HIPAA which set “Standards for Privacy of Individually Identifiable Health Information” found at 45 CFR Parts 160 and 164.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Request to Restrict Use and Disclosure of PHI (DHS 6240)

Replace with the actual printout of the form.

Request to Restrict Use and Disclosure of PHI by Parent, Guardian or Personal Representative (DHS 6241)

Replace with the actual printout of the form.



7 Business Associate Relationships

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part §164.502 (e) and §164.504 (e)(1)

Overview

The HIPAA Privacy Rule identifies a new category of business relationship, called a “business associate.” The Privacy Rule requires that a health plan covered by HIPAA, such as Medi-Cal, enter into a business associate contract in order to disclose protected health information (PHI) to the business associate.

To be a business associate, a contractor or agency partner:

- Must perform or assist in performing a function or activity which involves the use or disclosure of individually identifiable health information;
- Perform activities, such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management, and re-pricing on behalf of a Department of Health Services (DHS) health plan such as Medi-Cal; and
- Provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a DHS health plan such as Medi-Cal.

The following are not business associates or business associate relationships:

- DHS employees, divisions, and programs;
- Medical providers providing treatment to individuals;
- Another government agency performing enrollment or eligibility determinations involving Medi-Cal clients;
- Payment relationships, such as when Medi-Cal pays medical providers or other entities for services to Medi-Cal clients, when the other entity is providing its own normal services that are not on behalf of DHS, and

- When the only information being disclosed is information that is de-identified or not individually identifiable health information.

The Medi-Cal program may disclose an individual's PHI to a business associate and may allow a business associate to create or receive an individual's PHI from or on behalf of Medi-Cal, only when Medi-Cal has entered into a written agreement with the business associate. The written agreement must contain the terms specified below and must provide satisfactory assurance that the business associate will appropriately safeguard the information.

NOTE: A consultant working on a time and materials contract (hourly) may choose to have its employees complete the HIPAA Privacy Training if staff are working on-site and under the control of DHS, in lieu of signing a written business associate agreement.

This section explains the policies and procedures in the business associate relationship. The business associate section includes information pertaining to:

- Identifying and Tracking Medi-Cal Business Associates;
- Business Associate Agreements Compliance Dates;
- Required Terms and Conditions of Agreements;
- Business Associate is Another Government Entity;
- Response to Business Associate Inappropriate Uses or Disclosures; and
- Definitions.

Policy



The Medi-Cal program will enter into business associate contracts before disclosing PHI to its business associates. The purpose of this policy is to define Medi-Cal business associates, and to specify what provisions must be included in the Medi-Cal contracts with business associates and when they must be included.

Procedures



Each DHS health plan such as Medi-Cal covered by HIPAA must identify its business associates, contracts or inter-agency agreements with business associates, and renewal or amendment dates of these contracts and agreements. The following procedures will guide Medi-Cal in maintaining its business associate relationships.

Identifying and Tracking DHS Business Associates

The DHS Contract Management Unit (CMU) will notify each DHS health plan and provider covered by HIPAA of its obligation to incorporate business associate terms and conditions into DHS business associates' contracts and agreements and will monitor compliance with this obligation.

The CMU and the Medi-Cal program will not approve a new or amended contract or agreement with a business associate without the business associate terms and conditions. By April 14, 2004, all DHS business associate contracts and agreements will be amended to include standard business associate terms and conditions approved by the Privacy Officer and the CMU.

The Medical Care Services (MCS) Contract Officer and the Privacy Office maintain a list of all Medi-Cal contracts that include the HIPAA business associate language.

Compliance Dates

When the MCS enters into a new contract, renews an existing contract, or amends an existing contract with a business associate after October 15, 2002, business associate terms and conditions must be included in the contract.

All other contracts with business associates must be amended to include business associate terms and conditions by April 14, 2004.

Required Terms and Conditions

A contract between the Medi-Cal program and a business associate must include terms and conditions that establish the permitted and required uses and disclosures of PHI by the business associate. The contract may not authorize the business associate to use or further disclose the information obtained from Medi-Cal in a way that would violate the Privacy Rule, if done by Medi-Cal. However, the contract may permit the business associate to use and disclose PHI for its own proper management and administration and to provide data aggregation services relating to DHS health care operations.

In the Business associate Agreement, the business associate must agree to:

- Not use or further disclose PHI other than as permitted or required by the contract, or as required by law;
- Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for by the contract;
- Report to Medi-Cal and the Privacy Officer any use or disclosure not allowed by the contract of which it becomes aware;
- Ensure that any agents or subcontractors to which it provides PHI agree to the same restrictions and conditions that apply to the business associate under the contract;
- Make PHI available for inspection and copying to the individual in compliance with DHS policy and the Privacy Rule;
- Make PHI available for amendment and incorporate any amendments to PHI in accordance with DHS policy and the Privacy Rule;
- Make available the information required to provide an accounting of disclosures in accordance with DHS policy and the Privacy Rule;
- Make its internal practices, books, and records relating to the use and disclosure of PHI available to DHS and to the U.S.

Department of Health and Human Services for the purpose of determining DHS compliance with the Privacy Rule;

- At termination of the contract, if feasible, return and destroy all PHI that the business associate still maintains in any form, and keep no copies. If not feasible, continue to protect the information; and
- Authorize termination of the contract by DHS, if DHS determines the business associate has violated a material term of the contract.

Please note that there is a standard Business Associate Addendum which must be used for all Medi-Cal contracts with business associates, unless the Privacy Officer agrees to alternate language. (See Appendix)

Business Associate is Another Government Entity

If the Medi-Cal business associate is a governmental entity, Medi-Cal may enter into a memorandum of understanding or inter-agency agreement with the business associate which contains all the terms and conditions required by the Privacy Rule, except that it may omit the termination provision if this is inconsistent with statutory obligations of either agency.

If a governmental business associate is required by law to perform a function or activity on behalf of Medi-Cal, Medi-Cal may disclose PHI to the other agency to the extent necessary to comply with the legal requirement without a written contract or agreement:

- If other law or regulations applicable to the other agency accomplish the same objectives; or
- Medi-Cal documents its good faith attempts to obtain satisfactory assurances from the other agency its compliance with the business associate terms and conditions and the reasons such assurances cannot be obtained.

Please note that local County Welfare Departments performing enrollment eligibility determinations for Medi-Cal are specifically exempted by the Privacy Rule from the requirement of entering into business associate contracts with Medi-Cal.

Business Associate Non-Compliance

If the Medi-Cal program knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation under the contract or inter-agency agreement, Medi-Cal must:

- Ensure that the business associate takes reasonable steps to cure the breach or end the violation, including working with and providing consultation to the business associate;
- Terminate the contract, if such steps are unsuccessful; or
- If termination is not feasible, report the problem to the U.S. Department of Health and Human Services.

Response to Business Associate Inappropriate Uses or Disclosures

Business associate contracts require the reporting to DHS of any known inappropriate or unlawful use or disclosure of PHI within 24 hours of the contractor's discovery of the breach or sooner, if the breach is electronic or if computerized data. DHS employees may also receive a client complaint or report about inappropriate uses or disclosures of information by business associates.

DHS employees that receive a report from a business associate or any other person of a breach of security involving PHI or an inappropriate use or disclosure of such information by the business associate or a subcontractor of the business associate, should relay that report as soon as possible to the DHS Privacy Officer. The Privacy Officer will contact the contract manager, the business associate's or subcontractor's staff, and other appropriate authorities as necessary and conduct an investigation. The Privacy Officer will also require the business associate to conduct an internal investigation and report the results.

The Privacy Officer will coordinate with the business associate's DHS contract manager to document the alleged violation. If determined necessary and appropriate, DHS will generate a "cure" letter outlining required remediation in order for the business associate to prevent further breaches or unauthorized uses or disclosures of PHI. Please note that state law requires the notification of California residents when their names and social security numbers in electronic form are obtained by

unauthorized persons. This notification is the responsibility of the business associate. (See Privacy Breach section)

In cases where contract compliance cannot be attained, DHS must terminate the contract or agreement, if feasible. If termination is not feasible, the Privacy Officer will report the problem to the U.S. Department of Health and Human Services.

Definitions



Business Associate

Business associate means a person, entity, or contractor which is not a member of the workforce of the health plan but which arranges, performs, or assists in performing a function or activity involving the use or disclosure of PHI on behalf of the health plan.

Individually identifiable health information

Individually identifiable health information is information that identifies the individual or may be used to identify the individual, and contains detailed health information about persons, including such things as address, gender, age, and spoken language, etc. These data are created or received by a health plan, and describe what a person's physical and/or mental health is currently, has been in the past, or will be in the future, the provision of health care or payment of health care for the individual.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.



8 Accounting of Disclosures

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part §164.528

Information Practices Act (IPA)
CA. Civil Code §1798.25

Overview

Under 45 C.F.R. §164.528, an individual has a right to receive an accounting of disclosures of protected health information (PHI) made by a Department of Health Services (DHS) health plan such as Medi-Cal or its business associates in the six years prior to the date on which the accounting is requested, except for the following disclosures:

- To carry out treatment, payment, or health care operations;
- To individuals about themselves;
- Incident to a use or disclosure otherwise permitted;
- Pursuant to an authorization;
- To persons involved in the individual's care or to notify such persons;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials; and
- As part of a limited data set.

NOTE: The IPA requires a broader accounting of disclosures than HIPAA. Disclosures must be accounted for to other governmental agencies, even if arguably related to the operations of the health plan, unless there is an IPA statement provided to the beneficiary notifying him or her that the information may be disclosed. The Medi-Cal application form contains this IPA statement; therefore, Workers Compensation and Estate Recovery disclosures are not accountable disclosures of the Medi-Cal program.

This section explains the policies and procedures for allowing individuals to receive an accounting of disclosures of their PHI

made by the Medi-Cal program or its business associates. The Accounting of Disclosures Section includes information pertaining to:

- Accountable Disclosures;
- Allowable Disclosures;
- Time Period for the Accounting of Disclosure;
- Content of Accounting of Disclosures;
- Requesting an Accounting of Disclosures;
- Verification of Individual Identity;
- Verification of Address;
- Provision of the Accounting;
- Fees for the Accounting;
- Documentation;
- Suspension of the right to receive an Accounting of Disclosures;
- Format and Tracking of Accounting of Disclosures;
- Alternative Systems for Tracking Data;
- Staff Assigned to Oversee Accounting of Disclosures;
- Multiple Disclosures;
- Disclosures for Research;
- Definitions;
- Accounting of Disclosures Log;
- Request for an Accounting of Disclosures of PHI (DHS 6244); and
- Request for an Accounting of Disclosures of PHI by Parent, Guardian or Personal Representative (DHS 6245).

Policy



The policy of the Medi-Cal program is to provide individuals their maximum rights to an accounting of disclosures of their PHI under the law.

Accountable Disclosures

DHS must account for disclosures of PHI:

- For Court Orders, Court-Ordered Warrants, Subpoenas, Administrative Requests and Search Warrants;
- For Breaches or Unauthorized Disclosures;
- For Accountable Disclosures made by Business Associates;
- To Public Health Agencies;
- To Health Oversight Agencies;
- To Coroners;
- To Public Safety;
- To U.S. Department of Health and Human Services;
- For Research; and
- To Other Governmental Agencies (under the IPA).

Allowable Disclosures

HIPAA allows for a variety of disclosures of information. However, individual DHS health plans have their own laws and regulations pertaining to the disclosure of information. Medi-Cal allows disclosures only for purposes directly connected to the administration of the program, so most of the permissive disclosures under the HIPAA Privacy Rule are not allowable for the Medi-Cal Program. See section on Uses and Disclosures.

Time Period for the Accounting of Disclosures

Medi-Cal must document and maintain a listing of disclosures for six years from the date of disclosure by the program or by its business associates. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

Content of the Accounting of Disclosures

Medi-Cal must provide the individual with a written accounting, on request, that includes:

- The date of the disclosure;
- The name of the entity or person and title who received the PHI and the business address of such entity or person;
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure.

NOTE: Under the IPA, disclosures of information pertaining to crimes, offenders, and suspected offenders to law enforcement and disclosures to regulatory agencies of federal, state and local government are considered disclosures that must be accounted for. This means that Medi-Cal must account for disclosures to such agencies as the Federal Bureau of Investigations (FBI), Department of Justice (DOJ), etc.

Procedures



The following procedures should be used when individuals request an accounting of disclosures by Medi-Cal of their PHI.

Requesting an Accounting of Disclosures

All requests for an accounting of disclosures must be made **in writing** using DHS form 6244, which has been customized by the Medi-Cal program. The responsible Medi-Cal staff member for receiving and processing requests for disclosures will be the designated HIPAA Liaison of each unit or program.

Many of the Medi-Cal beneficiaries will be directed by their Notices of Privacy Practices to contact the Privacy Office at (916) 445-4646 for information regarding their privacy rights, including obtaining an accounting of disclosures.

Verification of Individual Identity

In order to ensure that DHS is protecting individual health information, individuals requesting an Accounting of Disclosures must verify their identities. Individuals will be requested to include their beneficiary ID number, date of birth, and date of death of the beneficiary, in probate cases. **A request for accounting of disclosures must also be accompanied by a photocopy of the California driver's license, an identification card issued by the Department of Motor Vehicles, or any other document that appears to be valid and establishes identity.** It is up to the individual program person designated to process Accounting of Disclosures requests to verify the identity of individuals requesting the accountings.

Documents containing signatures are preferable, since the signature on the request form may be checked against the identification card. The following additional documents may be considered:

- Copy of the Individual's Birth Certificate;
- Beneficiary ID Card;
- Managed Care Card; or
- State or Federal Employee ID Card/Check Cashing ID Card.

A notarized signature may be provided in lieu of a copy of one of the listed identifiers.

Address Verification

Individuals requesting to be sent accountings of disclosures by mail must also verify their address. Requestors must include proof of their address such as recent electricity, gas or phone bills, driver's license, rent receipt, or other documentation showing the requestor's name and address.

Provision of the Accounting

Medi-Cal must provide the individual with the accounting requested within 60 days. If unable to provide the accounting within 60 days, Medi-Cal may extend the time to provide the accounting by no more than 30 days for any archived records, provided that:

- Medi-Cal, within 60 days, provides the individual with a written statement of the reasons for the delay and the date by which the accounting will be provided; and
- Medi-Cal may have only one such extension of time for action on a request for an accounting.

Fees for the Accounting of Disclosures

Medi-Cal must provide the first accounting to an individual in any 12-month period without charge. Medi-Cal may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, which should be limited to not more than ten cents (\$0.10) per page, provided that Medi-Cal informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Documentation

Medi-Cal must document the following and retain the documentation:

- The information required to be included in an accounting;
- The written accounting that is provided to the individual under this section; and
- The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Medi-Cal must also ensure that its business associates which are delegated authority to make PHI disclosures keep equivalent records.

Suspension of the Right to Receive an Accounting of Disclosures

Medi-Cal must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides Medi-Cal with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the agency or official statement is made orally, Medi-Cal must document the statement, including the identity of the agency or official making the statement. The temporary suspension may be limited to no more than 30 days of the date of the oral statement.

Format for Maintaining an Accounting of Disclosures

Medi-Cal must establish a procedure for maintaining an accounting of all disclosures of PHI outside of the exceptions listed in this section.

Given the number of beneficiaries and the sophistication of the existing databases, Medi-Cal will need to decide how it can most efficiently track the required information, unless and until DHS establishes a centralized system for tracking disclosures of PHI. Medi-Cal must also ensure that business associates, such as Electronic Data Systems (EDS), which disclose PHI, establish such procedures.

Alternative Systems for Tracking Data

An existing database may be edited to provide for entry of the disclosures and all required information attached to the beneficiary file. Some options for tracking data are:

- Attach hard copy to paper beneficiary file;
- Hard Copy List;
- Excel spreadsheet; or
- Access Database developed.

Staff Assigned to Oversee Accounting of Disclosures

A staff person must be assigned the responsibility for collection and maintenance of accounting of disclosure information. The name of this person should be forwarded to the DHS Privacy Office at **PrivacyOfficer@dhs.ca.gov**.

Staff will report each disclosure to the assigned person for tracking.

The Medi-Cal program will send a copy of the Accounting of Disclosures Log to the Privacy Office quarterly (calendar year). All breaches, which will be reported to the Privacy Office upon their occurrence, should be included in the accounting of disclosures.

Multiple Disclosures

If, during the period covered by the accounting, Medi-Cal has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:

- The information required above under “Content of Accounting of Disclosures” for the first disclosure during the accounting period;
- The frequency, periodicity, or number of the disclosures made during the accounting period; and
- The date of the last such disclosure during the accounting period.

Disclosures for Research

If, during the period covered by the accounting, Medi-Cal has made disclosures of PHI for a particular research project determined to be directly connected with the administration of the program for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

- The name of the protocol or other research activity;
- A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

- A brief description of the type of PHI that was disclosed;
- The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
- The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the information was disclosed; and
- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If Medi-Cal provides an accounting for research disclosures, and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, Medi-Cal should, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

Definitions



Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Use

Use is the sharing, application, utilization, examination, or analysis of PHI within a covered health plan or provider which maintains the information.

Disclosure

Disclosure is the release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

Accounting of Disclosures Log

Program:

Date: _____ Quarter of 20_____

[illegible]

Request for an Accounting of Disclosures of PHI (DHS 6244)

Replace with actual form.

Request for an Accounting of Disclosures of PHI by Parent, Guardian or Personal Representative (DHS 6245)

Replace with actual form.



9 Amending Protected Health Information

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR §164.526

Information Practices Act (IPA)
CA Civil Code §§1798.35, .36, and .37

Overview

Federal and state laws mandate that the Department of Health Services (DHS) ensure that an individual has the right to request amendment of his or her health information. The Medi-Cal program recognizes that individuals have the right to request, in writing, that an amendment be made to their protected health information (PHI) and records about them in a designated record set for as long as the designated record set is maintained by Medi-Cal.

This section establishes the policy and procedures for receiving and processing requests for amendment of PHI. This section includes information pertaining to:

- Timely action – within 30 days of receipt of request;
- Verification of individual identity of requester;
- Personal representative requests;
- Address verification;
- Denying the amendment;
- Review of refusal to amend record;
- Statement of disagreement of requester;
- Rebuttal statement;
- Amendments forwarded to prior covered entities;
- Definition of terms;
- Request to Amend PHI (DHS 6238); and
- Request to Amend PHI by Parent, Guardian or Personal Representative (DHS 6239).

Policy



The Medi-Cal program recognizes that individuals have the right to request, in writing, an amendment be made to their PHI and records about them in a designated record set for as long as the designated record set is maintained by Medi-Cal or its business associates.

Procedures



Medi-Cal will make the amendment to the PHI or record that is the subject of the request for amendment, if appropriate, by identifying the records in the designated record set that are affected by the amendment and appending or providing a link to the location of the amendment. Upon acceptance of the amendment, Medi-Cal will ask the individual to whom he or she wants the amendment sent. Medi-Cal will send the amendment to any persons identified by the individual and any covered entities or business associates to which Medi-Cal has previously sent the individual's PHI.

Individuals may request amendments when they believe any portion of a record is not accurate, relevant, timely or complete. (IPA §1798.35 (a)).

The following procedures should be used to comply with the requirement to make amendments to PHI.

Timely Action

Medi-Cal will make the amendments to the PHI or mail a denial of the request to amend within 30 days of receipt of the request. The request should be received on the Medi-Cal Request to Amend PHI form (DHS 6238), accompanied by proper identification and address verification.

Verification of Individual Identity of Requester

In order to ensure that DHS is protecting individual health information, individuals requesting to inspect and copy records must verify their identities. Individuals will be requested to include their beneficiary ID number, date of birth, and date of death of the beneficiary, in probate cases. A photocopy of the California driver's license, an identification card issued by the

Department of Motor Vehicles, or any other document that appears to be valid and establishes identity, must also accompany a request to amend. It is up to the individual program person designated to process access requests to verify the identity of individuals requesting access or amendments to their own records. Documents containing signatures are preferable, since the signature on the request form may be checked against the identification card. The following additional documents may be considered:

- Copy of the Individual's Birth Certificate;
- Beneficiary ID Card;
- Managed Care Card; or
- State or Federal Employee ID Card/Check Cashing ID Card.

A notarized signature may be provided in lieu of a copy of one of the listed identifiers.

Personal Representative Request

When a personal representative requests access to records of an individual or requests amendments be made to that individual's records, his or her legal authority to make medical decisions must be verified as well as his or her identity, using the above process. Verification of legal authority to make health care decisions would include documentation establishing conservatorship, legal guardianship, or power of attorney for health care decision-making. A copy of the death certificate should be required in the case of the records of decedents, as well as proof of executorships of the will/ administration of the estate. If the estate did not go through probate, proof of status as the next of kin (e.g. spouse or child) of the decedent may be sufficient.

Address Verification

Individuals requesting to amend records by mail must also verify their address. Requestors must include proof of their address such as recent electricity, gas or phone bills, driver's license, rent receipt, or other documentation showing the requestor's name and address.

Denying the Amendment

The amendment request will be denied if the Medi-Cal program determines that:

- The PHI or record that is the subject of the request was not created by Medi-Cal, unless the individual proves that the originator of the PHI can no longer act on the requested amendment;
- The PHI or record that is the subject of the request is not part of the designated record set;
- The individual was denied access to the information previously or would have been denied access if he or she requested it; and
- Medi-Cal believes the information is accurate and complete.

Medi-Cal will give the individual a written denial that includes, in plain language:

- The basis for the denial;
- The individual's right to request a review of the refusal to amend a record by an official designated by DHS;
- The individual's right to submit a written statement disagreeing with the denial and how to file the statement;
- A statement that with any future disclosures of PHI, DHS will include the request for amendment, the denial, the individual's statement of disagreement (if any), and the rebuttal statement (if any);
- The process for complaining to the DHS Privacy Officer; and
- A description of how the individual may complain to the Secretary of the U.S. Department of Health and Human Services.

Medi-Cal will append or link to the identified PHI or record that is the subject of the amendment the following information to the designated record set:

- The individual's request for amendment;
- DHS denial of the request;
- The individual's statement of disagreement (if any);

- DHS rebuttal statement (if any); and
- The review of the refusal to amend the record (if any).

Review of Refusal to Amend Record

Under section 1798.36 of the IPA, individuals may request a review of a refusal to amend the record by the director of DHS or official designated by the Director. The agency's decision must be made no later than 30 days from the date on which the individual requests the review. If the reviewing official refuses to amend the record, the individual may file a statement of disagreement with the agency.

Statement of Disagreement of Requester

DHS permits individuals to submit a written statement of reasonable length disagreeing with the denial of all or part of the requested amendment and the basis for such disagreement.

Rebuttal Statement

DHS may prepare a written rebuttal to the individual's statement of disagreement. If a rebuttal is prepared, DHS will provide a copy to the individual.

Amendments Forwarded by Prior Covered Entities

When Medi-Cal receives an amendment to PHI from another covered entity, which is the originator of PHI, Medi-Cal will append or link the amendment to the designated record set.

Definitions



Designated Record Set

Designated record set is a group of records maintained by or for the Medi-Cal program that is:

- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for Medi-Cal; and/or
- Used, in whole or in part, by or for the Medi-Cal program to make decisions about individuals.

Individually Identifiable Health Information

Individually identifiable health information is information that identifies the individual or may be used to identify the individual, and contains detailed health information about persons, including such things as address, gender, age, and spoken language, etc. These data are created or received by a health plan, and describe what a person's physical and/or mental health is currently, has been in the past, or will be in the future, the provision of health care or payment of health care for the individual.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Request to Amend PHI (DHS 6238)

Replace with actual form.

Request to Amend PHI by Parent, Guardian or Personal Representative (DHS 6239)

Replace with actual form.



10 Confidential Communications

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part §164.522 (b)

Overview

The Medi-Cal program must permit individuals to request and must accommodate reasonable requests to receive communications of protected health information (PHI) by alternative means or at alternative locations if the individual clearly states that the disclosure of the PHI could endanger him or her.

For example, an individual who does not want his or her family members to know about certain treatment may request that Medi-Cal communicate with the individual about treatment or payment at the individual's place of employment, by mailing to a designated address, or by calling a designated phone number, such as a cell phone.

For example, an individual requests that Medi-Cal mail explanations of benefits about particular services to the individuals' work rather than home address, because the individual is concerned that a member of the individual's household might read the explanation of benefits and become abusive towards the individual. Medi-Cal must accommodate the request.

The reasonableness of a request made by the individual must not be determined by Medi-Cal solely on the basis of the administrative difficulty of complying with the request.

This section explains the Medi-Cal policy regarding confidential communications and the procedures used to accommodate these requests. The Confidential Communications section includes:

- Requesting Confidential Communications;
- Alternative Address and/or Alternative Telephone Number Request;
- Alternative Means of Contact;

- Approving or Denying the Request;
- Definitions; and
- Confidential Communication Request form (DHS 6235)

Policy



Medi-Cal will accommodate reasonable requests by beneficiaries to be contacted by alternative means or at alternative locations if a beneficiary requests confidential communications and states that disclosure of information by regular means could be a danger to him or her.

Procedures



The following procedures should be used to process requests for confidential communications.

Requesting Confidential Communications

An individual must make their request for alternative methods of communications in writing or complete a Confidential Communications Request form (DHS 6235).

Individuals must provide the alternative address or telephone number at which they wish to be contacted, along with a written statement that receiving mail or a telephone call at the address or phone number listed on the individual's record may jeopardize the individual's safety.

If an individual is asking for all Medi-Cal information to be sent to an alternative address, he or she should be directed to the county eligibility worker for a change of address. If beneficiaries want an alternative phone number to be used in particular circumstances then they should be given the Privacy Office number and told to choose the Medi-Cal Line which will direct them to Electronic Data Systems (EDS), which will send them the form for alternative method of communication. The number is 916-445-4646.

Alternative Address and/or Alternative Telephone Number Request

Individuals must submit requests in writing or fill out a Confidential Communications Request form (DHS 6235). If the individual sends a request in writing, the following information must be provided:

- Alternative Address and/or Alternative Telephone Number, including City, State, Zip;
- Current Address and/or Telephone Number, including City, State, Zip;
- Signature;
- Signature of personal representative, if applicable;
- Date Signed; and
- Statement declaring contacting the individual at the current address and/or telephone number could endanger the individual. Details are not required.

Alternative Means of Contact

If an individual requests to be contacted by an alternative means, Medi-Cal must look at the reasonableness of the request. In general, Medi-Cal will not be able to agree realistically to contact individuals only by telephone. There may be some exceptions, such as Family PACT. A client may request not to be contacted by telephone. If so, this notation should be accommodated, unless it is unreasonable, given the circumstances of the program, and the notation made in the appropriate file.

Approving or Denying the Request

When a request for alternative method of communications is received, the Medi-Cal program should review the request to ensure that a safety issue is clearly stated and to determine the reasonableness of the request. The individual does not have to explain the safety reason. Reasonableness should be determined based on whether Medi-Cal would be prevented from conducting business as usual and whether an undue workload is created.

If the individual provides a safety reason and an alternative method of contact, which is reasonable, the request should be granted in most cases.

If Medi-Cal approves the request for confidential communications, the approval should be in writing and sent to the alternative address provided, kept in the individual's file, or noted on the electronic record and centralized in a file. Any mailing lists must be updated with the new information immediately.

If Medi-Cal denies the request for alternative method of contact, Medi-Cal should attempt to call the individual via the current telephone number and notify the individual of the denial. If a telephone number is not available, Medi-Cal should send a letter to the individual at the current address.

Definitions



Individually Identifiable Health Information

Individually identifiable health information is information that identifies the individual or may be used to identify the individual, and contains detailed health information about persons, including such things as address, gender, age, and spoken language, etc.

These data are created or received by a health plan, and describe what a person's physical and/or mental health is currently, has been in the past, or will be in the future, the provision of health care or payment of health care for the individual.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Confidential Communication Request (DHS 6235)

Replace with actual form



11 Complaints

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR §164.530(d)

Overview

Federal law mandates that the Department of Health Services (DHS) ensure that employees, staff of its business associates, and individual patients or other persons have the right to file a complaint concerning the policies and procedures required by the HIPAA Privacy Rule developed by a health plan or provider or compliance with those policies and procedures and the HIPAA Privacy Rule by a health plan or provider.

Complaints may be received from:

- DHS employees;
- Staff of its business associates;
- Individual program beneficiaries/patients; and
- Other persons.

This section explains the DHS policy regarding privacy complaints and the procedures used to address the complaint. The Complaint section includes:

- Who May File a Complaint;
- Time Limits for Filing Complaints;
- Complaint Form (DHS 6242) and Whistleblower Form (DHS 6243) Process;
- Submitting the Complaint;
- Initial Analysis and Routing of Complaint;
- Investigating and Resolving Complaints;
- Complaint Status Log;
- Retaliation;
- Documentation;
- Definitions;

- Privacy Complaint Form (DHS 6242); and
- Whistleblower Complaint Form (DHS 6243).

Policy



DHS will accept complaints from its employees, staff of its business associates, and individual program beneficiaries/patients or other persons concerning the DHS policies and procedures required by the HIPAA Privacy Rule and compliance with those policies and procedures; investigate alleged violations; and resolve the issues raised in order to safeguard an individual's protected health information (PHI) and improve the DHS business systems and practices.

Procedures



The following procedures should be used to notify individuals of their right to complain and to accept and resolve the complaint in a timely manner.

Who May File a Complaint

Through its Notices of Privacy Practices, automated phone answering system, and internet and intranet web sites, DHS informs individual program beneficiaries/patients, the public, and whistleblowers of their right to file a complaint with either the Department or the Secretary of the U.S. Department of Health and Human Services (DHHS). The Privacy Officer supervises the DHS complaint process. The Privacy Officer will receive telephonic and written complaints with respect to privacy from:

- Individuals whose PHI DHS maintains, or other persons regarding suspected violations of the Privacy Rule by DHS.
- Whistleblowers - DHS employees and employees of the DHS business associates may file complaints regarding suspected violations of HIPAA privacy requirements by another Department employee, or about the DHS privacy policies and procedures.

Time Limits for Filing Complaints

An individual program beneficiary/patient or others must file a written complaint, either on paper or electronically, within 180 days of when the complainant knew or should have known of the alleged violation. There is no time limit for a whistleblower to file a written complaint. Some complaints will be accepted by telephone, such as anonymous complaints and complaints by those needing translation services.

Complaint Forms

The complaint should be made on the DHS Complaint Form (DHS 6242). Whistleblowers should use the Whistleblower Complaint Form (DHS 6243). However, any written complaint containing the information required below will be accepted. The written complaint should include the following:

- Be addressed or directed to the Privacy Officer;
- The name of the organization the complaint is filed against, the name of the person the complaint is filed against, date the violation was first noticed, and the date(s) the violation(s) occurred;
- The nature of the violation, i.e.:
 - PHI inappropriately disclosed;
 - PHI inappropriately used;
 - PHI inappropriately discarded;
 - Denial of access to PHI;
 - Denial of amendment to PHI;
 - Other denial of privacy rights;
 - DHS privacy policies and procedures violate HIPAA requirements; and
 - Retaliatory or intimidating actions.
- Detailed description of the complaint;
- Witnesses, if any;
- Possible resolution of the complaint;

- Optional information, i.e.:
 - Name and address of complainant (complaints may be filed anonymously);
 - Consent to disclose complainant's name during investigation;
 - Complainant's signature; and
 - Consent to refer complaint to other agencies.

Submitting the Complaint

The Complaint form (DHS Form 6242) may be mailed to DHS at:

Department of Health Services
Privacy Office - MS 0010
PO Box 99743
Sacramento, CA 95899-7413

Some complaints will be accepted by telephone, particularly when there is a need for language translation services.

Initial Analysis and Routing of the Complaint

Upon receipt, Privacy Office staff will enter the required information on the HIPAA Privacy Complaint Status Log within 2 business days of receipt or assignment. The Privacy Office will verify the alleged violation(s) occurred after April 13, 2003, and fits one of the following categories:

- PHI inappropriately disclosed;
- PHI inappropriately used;
- PHI inappropriately discarded;
- Denial of access to PHI;
- Denial of amendment to PHI;
- Other denial of privacy rights;
- DHS privacy policies and procedures violate HIPAA requirements; or
- Retaliatory or intimidating actions.

If the complaint is not related to any of the above and/or does not relate to a DHS health plan or provider, the Privacy Office will prepare a letter acknowledging receipt of the complaint with an explanation of why the complaint will not be investigated. The action will be noted on the Status Log. With the consent of the complainant, the Privacy Office will refer complaints to other appropriate agencies with jurisdiction to investigate the complaint and take enforcement action.

Privacy complaints against providers of DHS programs which appear to be valid, after initial review, will be handled by sending a letter to the provider, reminding the provider of any legal obligation to comply with State and federal privacy laws. A referral will be made to the federal Office for Civil Rights for complaint investigation and enforcement, if the complainant agrees.

If the alleged violation is the inappropriate use or disclosure of PHI, the Privacy Office will check the rules for the program involved on uses and disclosures. If the alleged violation was an allowable use or disclosure, the Privacy Office will prepare and mail, if applicable, a letter acknowledging receipt of the complaint and explain that the use or disclosure was allowable under HIPAA and other applicable law.

If the Privacy Office determines that the complaint is valid, staff will investigate it, under the supervision of the Privacy Officer, and in consultation with the DHS health plan or provider, if necessary. The Privacy Office will prepare and mail, if applicable, a letter acknowledging receipt of the complaint.

Investigating and Resolving Complaints

The investigative team may include members of the Privacy Office, the DHS Audit and Investigations Division, and the staff of the program complained against, if appropriate.

The strategy used to investigate the complaint may include:

- Interviews with staff who allegedly violated HIPAA;
- Review of staff's behavior with supervisor or management team;
- Review of the business practices that resulted in the alleged violations and discussion with appropriate management team;

- Review of the business associate's conduct and the business associate's contract, if applicable; and
- Interviews with witnesses and examination of documents relevant to the complaint.

Resolution of the complaint may include recommendations to:

- Change business practices;
- Provide additional training to staff;
- Discipline staff;
- Require a compliance plan for business associate contractor; and
- Terminate the contractor.

If the investigation results in findings of harmful effects to the complainant, the Privacy Officer's recommendations for mitigating the harmful effects may include a letter of apology, appropriate remediation measures to benefit the complainant and other appropriate measures.

Status Log

Upon notification of the final resolution of a complaint, the Privacy Office staff will enter the information on the status log and send a letter to the complainant of the final outcome of the complaint.

Retaliation

Employees of DHS will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person for:

- Filing a complaint with DHS or the Secretary of the Department of Health and Human Services;
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or
- Opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve the disclosure of PHI.

DHS will train its staff on this non-retaliation policy. Supervisory staff will receive training on how to effectively deal with individuals who believe retaliatory actions have been taken against them.

Documentation

The individual's complaint, any correspondence between DHS and the individual, and any documents generated by the investigation and resolution of the complaint, including mitigating harmful effects, will be retained for six years.

Definitions



Individually Identifiable Health Information

Individually identifiable health information is information that identifies the individual or may be used to identify the individual, and contains detailed health information about persons, including such things as address, gender, age, and spoken language, etc.

These data are created or received by a health plan, and describe what a person's physical and/or mental health is currently, has been in the past, or will be in the future, the provision of health care or payment of health care for the individual.

Protected Health Information

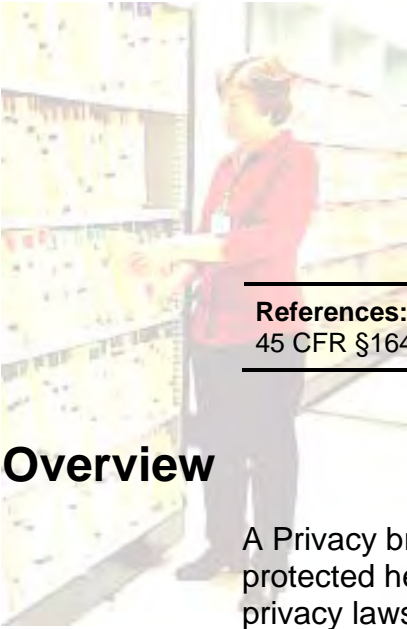
PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

Privacy Complaint Form (DHS 6242)

Replace with actual form

Whistleblower Complaint Form (DHS 6243)

Replace with actual form



12 Privacy Breach

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR §164.504; Civil Code §§1798.29 and .82

Overview

A Privacy breach is an unauthorized use or disclosure of protected health information (PHI) that violates state or federal privacy laws, such as the HIPAA Privacy Rule.

In the event of a privacy breach, Department of Health Services (DHS) staff should immediately report the breach to the DHS Privacy Officer.

The HIPAA Privacy Rule requires that business associates of health plans notify the health plan of any instances of which they are aware that confidentiality of PHI has been breached.

Further, under state law, DHS must disclose any breach of the security of a computerized system that includes the name of an individual plus the social security number, driver's license number, California ID number or financial account number, to any resident of California whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

The DHS Privacy Officer and the Information Security Officer supervise the breach investigation process. The Privacy Office will assist in tracking and investigating breaches as necessary.

This section explains the guidelines to be followed in the event of a breach of privacy. The privacy breach section includes:

- Who May Notify of a Breach;
- Breach Notification Process;
- Initial Analysis of a Breach;
- Investigating and Resolving Breaches;
- Retaliation;
- Documentation; and

- Definitions.

Policy



DHS will investigate all alleged breaches of PHI reported by its employees, staff of its business associates, and individual program beneficiaries/patients or other persons; and will work to resolve the issues raised in order to safeguard an individual's PHI and improve the DHS business systems and practices.

Procedures



The following procedures should be used to ensure appropriate investigation, mitigation, and corrective action when DHS is made aware of a privacy breach.

Who May Notify of a Breach

An individual whose PHI DHS maintains, a member of the DHS workforce, or a member of a business associate's workforce, or other persons, may notify the Privacy Officer and/or the Information Security Officer of alleged breaches of PHI maintained by DHS.

Breach Notification Process

- DHS employee or business associate must provide notice to the contract manager, the DHS Privacy Officer and the DHS Information Security Officer within one hour (1) hour, either on paper or electronically, of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable Federal and State laws or regulations
- If the breach involves electronic PHI, the originator of the breach may have to notify all individuals whose information was included in the breach, if the requirements of Civil Code §§1798.29 and .82 are triggered.

- The breach notification must include all of the following:
 - Be addressed or directed to the contract manager, the DHS Privacy Officer and the DHS Information Security Officer
 - The name of the organization in which the alleged breach occurred, the name of the person reporting the alleged breach, the date the violation was first noticed, and the date(s) the violation(s) occurred.
 - The nature of the violation:
 - PHI inappropriately disclosed;
 - PHI inappropriately used; or
 - PHI inappropriately discarded;
 - Detailed description of the alleged breach.
 - Witnesses, if any.
 - If the alleged breach occurs with a DHS business associate, the business associate should conduct an investigation and provide a written report of the investigation to the DHS Privacy Officer within ten (10) working days of the discovery of the breach or unauthorized use at the address or email listed below:

Department of Health Services
Privacy Office
P.O. Box 997413, MS 0010
Sacramento, CA 95899-7413

Initial Analysis of the Breach

- Upon notification of an alleged breach from a DHS business associate, DHS staff should ensure that the notification process referenced above is followed.
- The Privacy Officer should be notified via telephone or email.
- Privacy Office staff will enter the required information on the HIPAA Privacy Breach/Complaint Tracking Log.
- Privacy Office staff will complete a Breach Tracking Form and retain copies of all documents.

- DHS Program staff will send all information to the Privacy Officer.
- Privacy Office staff will work closely with the DHS program to ensure the following steps are completed:
 - Complete investigation by the party responsible for the breach (business associate or program management).
 - Mitigation activities, including any legally required notification to beneficiaries.
 - Formal Corrective Action Plan.
 - Remediation Efforts.
 - Follow up to ensure all resolution activities are completed.

Investigating and Resolving Breaches

The investigative team for breaches may include, but is not limited to, members of the Privacy Office, the DHS Audit and Investigations Division, the Information Security Office and DHS program staff involved with the business associate, and business associate workforce members, if appropriate.

The strategy used to investigate the breach may include but is not limited to:

- Meetings with those involved with the breach;
- Review of the business practices that resulted in the alleged violations and discussion with appropriate management team;
- Review of the business associate's conduct and the business associate's contract; or
- Interviews with involved employee (s);

Resolution of the breach may include recommendations to:

- Change business practices;
- Provide additional training to staff;
- Discipline staff;
- Require a compliance plan for business associate contractor; and

- Terminate the contractor.

Business associates should take prompt corrective action to cure any deficiencies and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations, including notification to beneficiaries.

If the investigation results in findings of harmful effects to individual(s), the Privacy Officer's recommendations for mitigating the harmful effects may include:

- A letter of apology.
- A letter notifying individuals of the breach, even if paper, and advising how to protect against identity theft (when it appears that unauthorized persons with malicious intent have acquired the PHI).
- Appropriate remediation measures to benefit the individual(s).
- Other appropriate measures.

Retaliation

Employees of DHS will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person for:

- Notifying DHS of an alleged breach; or
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing.

DHS will train its staff on this non-retaliation policy. Supervisory staff will receive training on how to effectively deal with individuals who believe retaliatory actions have been taken against them.

Documentation

All documentation relevant to the breach and any documents generated by the investigation and resolution of the breach, including mitigating harmful effects, will be retained for six years. The Privacy Office will complete documentation and all privacy breach documentation will be retained in the DHS Privacy Office.

Definitions



Privacy Breach

Privacy breach is an unauthorized use or disclosure of PHI that violates state or federal privacy laws, such as the HIPAA Privacy Rule.

Privacy Rule

The Privacy Rule is regulations implementing the HIPAA which set “Standards for Privacy of Individually Identifiable Health Information” found at 45 CFR Parts 160 and 164.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.

13 Training

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part §164.530 (b) (1)

Overview

The HIPAA Privacy Rule requires the Department of Health Services (DHS) to train all members of its workforce on privacy policies and procedures with respect to protected health information (PHI), as necessary and appropriate for members of the workforce to carry out their functions within the DHS health plans.

The Training Section includes:

- Mandatory Training Information;
- Changes to Privacy Policies and Procedures;
- Method of Training;
- Content of Training;
- Documentation to be Maintained; and
- Definitions.

Policy



DHS must train new staff within 30 days of their start date. The new staff, including new state employees, state employees new to DHS and state employees new to the Medi-Cal Program will be trained in both HIPAA Awareness and HIPAA Medi-Cal Policies and Procedures. Medical Care Services (MCS) will aim to train new employees within 30 days of their start date. Contractual staff and consultants who work on-site and under the control of DHS, student interns and volunteers are considered members of the DHS workforce and will also be trained.

Mandatory Training Information

The HIPAA Privacy Rule requires that work force members be trained to the extent they perform functions covered by the Privacy Policies and Procedures.

Workforce includes all employees, trainees, students, and interns, paid and volunteer, who perform services for DHS. It does not include staff of DHS business associates, such as Electronic Data Systems (EDS), Delta Dental, etc., which perform functions under contract for Medi-Cal covered programs. HIPAA requires that DHS train members of its workforce to the degree “necessary and appropriate for the member of the workforce to carry out their functions...” The Privacy Office approach to training will take into account the location of employees in a covered or non-covered program and the specific role of groups of employees.

DHS Privacy Office training, including HIPAA Awareness and Medi-Cal Privacy Policies and Procedures, will incorporate the following:

- The federal HIPAA Privacy Rule;
- The interaction between the HIPAA Privacy Rule and the federal and state privacy laws and regulations that govern the Medi-Cal program;
- The administrative requirements of HIPAA for health plans; and
- Medi-Cal Privacy Policies and Procedures.

Medi-Cal managers will be expected to implement and monitor on-going training of new employees, with assistance, if required, by the Privacy Office.

Changes to Privacy Policies and Procedures

Medi-Cal must train its workforce on changes to HIPAA Medi-Cal Privacy Policies and Procedures within a “reasonable time”.

The HIPAA Privacy Rule requires DHS to train its workforce initially and when changes occur in the privacy policies and procedures. This would include when the U.S. Department of Health and Human Services makes changes to the privacy regulations and when the DHS Privacy Office makes changes to

its privacy policies and procedures or Medi-Cal changes its own privacy policies and procedures.

The DHS Privacy Office will provide training on privacy policies and procedures to incorporate changes made by the federal government, revisions to DHS policies, and as a means to keep DHS employees aware of the importance of these privacy policies and procedures.

Procedures



The following procedures should be followed to ensure Medi-Cal staff is trained in both the Privacy Rule and Policies and Procedures.

Method of Training

HIPAA Awareness training is completed via the web-based training presentation. The Privacy Office will conduct policy and procedure training for the Medi-Cal program. This level of training will include a hands-on look at forms and procedures for the use and disclosure of PHI, including elements such as the verification of identity for those requesting access to PHI. The Privacy Office will also conduct specific training for internal business associates of the Medi-Cal program such as Audits and Investigations, Office of Legal Services, Accounting, and Information Technology.

External business associates are organizations acting on behalf of DHS who use PHI. DHS expects its business associates to train their workforce. DHS is not responsible for providing training to business associate employees, but may provide training to business associates to enable them to fulfill their obligations, such as providing access to PHI to program recipients. Training will initially include the provision of scripts to answer anticipated questions and an overview of the new HIPAA compliance forms, (i.e., access to records, amendments, and complaints).

Content of Training

Federal law requires that privacy training be specific to DHS Policies and Procedures, not merely a recitation of the Privacy Rule. HIPAA Awareness Training lays out the rights of DHS

health plan recipients and the responsibilities of DHS health plans and providers in ensuring these rights. In Medi-Cal Policies and Procedures Training employees will be given information on the Medi-Cal Privacy Policies, a synopsis of the Medi-Cal Policies and Procedures, where to get more information if they have questions on privacy policies and/or procedures, what their responsibilities are in protecting the privacy of health information, and the sanctions that may be imposed for violation of these policies and procedures.

Documentation to be Maintained

Since training is a required activity under the Privacy Rule, the documentation of training must be in a written or electronic record, and include the type of training, when it was conducted, and who received it. The Privacy Office and the Medi-Cal program should maintain the documentation of training for six years from the date of its creation or the date it was last in effect, whichever is later.

Documentation of department-wide training will reside with the Privacy Office. The user ID will be used to track which members of the workforce have and have not been trained. This information will be stored in a database. These records will be maintained for six years.

After completing the HIPAA Awareness Training, DHS workforce members will be asked to print out and sign a document certifying they understand the Privacy Rule and the Privacy Policies and Procedures. These certifications should be given to their managers or supervisors and stored in the supervisor's informal employee files.

Upon completion of the Medi-Cal Policies and Procedures Training, DHS workforce members will receive a Certificate of Completion by either the Privacy Office or the Program Managers, whoever gives the training. Documentation of training completion should be maintained in Medi-Cal employees' files.

Definitions



Privacy Rule

The Privacy Rule is regulations implementing HIPAA which set “Standards for Privacy of Individually Identifiable Health Information” found at 45 CFR Parts 160 and 164.

Protected Health Information

PHI is individually identifiable health information that describes the past, present, or future physical or mental health or the condition of an individual. PHI includes information about the health care services an individual has received or will receive and information about payment for health care services provided in the past, present, or future.



14 Employee Sanctions

References: Health Insurance Portability and Accountability Act (HIPAA)
45 CFR Part §164.530 (e)

Information Practices Act (IPA)
CA Civil Code §§1798.53, .55, and .57; Welfare and Institutions Code
§14100.2

Overview

The HIPAA Privacy Rule (Privacy Rule) requires that the Department of Health Services (DHS) have and apply appropriate sanctions to members of its workforce who fail to comply with the Privacy Policies and Procedures or the requirements of the Privacy Rule. [45 C.F.R. §164.530(e)(1)]

This section explains the DHS policy regarding employee sanctions for failure to comply with the HIPAA Privacy Rule and other privacy laws and regulations. The Employee Sanction section includes:

- Tracking Privacy Violations;
- Responsibilities of Managers and Supervisors;
- Training and Certification; and
- Criminal and Civil Penalties.

Policy



DHS employees who violate the program privacy policies and procedures or the Privacy Rule will be subject to the State Progressive Discipline Process. Please refer to the Preventive, Corrective, and Adverse Actions Handbook.

Managers and supervisors must ensure that employees are trained on the Privacy Rule and on program privacy policies and procedures, which apply to their job functions.

Sanctions may include:

- Mandatory Training;
- Disciplinary Actions; and
- Termination.

Procedures



The following procedures should be used to impose sanctions on employees who violate the Privacy Rule or the DHS Policies and Procedures.

Violations

Violations include non-compliance with the Privacy Rule, the DHS Privacy Policies and Procedures, any privacy process implemented by the individual program, or other state or federal laws which apply to privacy.

Tracking Privacy Violations and Applied Sanctions

Documentation of violations and the sanctions applied must be sent to the Privacy Office in order to meet tracking requirements under the Privacy Rule. Violations will be stored in a secure database to be used in reporting to the U.S. Department of Health and Human Services.

Responsibilities of Managers and Supervisors

Managers and supervisors will investigate and document the non-compliance of their staff members. All documentation, including sanctions, will be sent to the Privacy Officer. Managers may utilize the Privacy Officer to help determine the severity of the infraction and the sanction placed on the staff member.

Managers and supervisors must ensure that employees are trained on the Privacy Rule and on DHS and program privacy policies and procedures, which apply to their job functions.

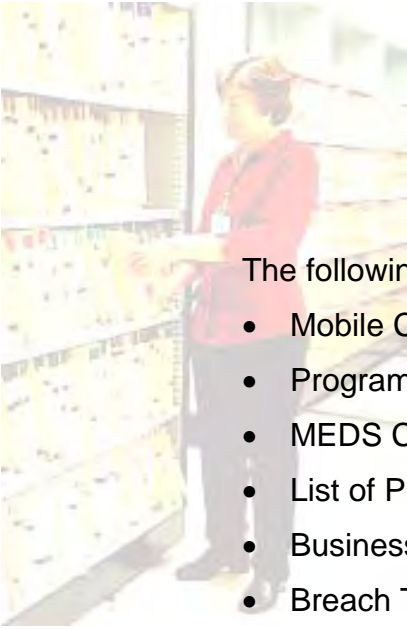
Training and Certification

DHS staff will be trained in both HIPAA Awareness and the Privacy Policies and Procedures. Certificates will be stored in the employee's personnel file.

DHS requires employees to sign a document certifying that they understand DHS Sanctions Policy and have been trained in the Privacy Rule.

Criminal and Civil Penalties

DHS employees should be aware that civil and criminal sanctions exist for violation of privacy laws by governmental employees and others. For violations determined to be sufficiently serious, employees may be referred for criminal prosecution. See Information Practices Act, Civil Code §§1798.53, .55 and .57 and Welfare and Institutions Code §14100.2.



Appendix

The following attachments appear in this Appendix:

- Mobile Computing Policy;
- Program Minimum Necessary Charts;
- MEDS Confidentiality Statement;
- List of Program Business Associates;
- Business Associate Agreement Template;
- Breach Tracking Form; and
- CA Civil Code §§1798.29 and 1798.82, .83 and .84.